Information Resource Review

Databases

- Which database systems do you currently operate?
- Which versions are currently using
- Are any of the systems end of vendor support
- What are the current database patch levels
- Is database logging enabled
- How often are databases updated
- Who has access to the root password accounts on the database servers?
- Can you provide a list of all database users with DBA access
- Can you provide a list of all database users with account status and privileges
- Can you provide evidence of the length of passwords, date of last password change, password complexity rule, date password is allowed
- How many oracle instances are needed for banner
- How are passwords stored (encryption format), please provide a list
- Are system passwords updated when users leave
- Do any of the users login as Oracle/Sysadm/
- Is there a process in place to log all scripts ran on the database system

Servers

- OS version for windows servers
- OS versions for Linux/Solaris server
- What are the update levels for the Linux/Mac vers
- What are the update levels for the Windows vers
- Are administrative passwords stored in a password manager
- Are passwords changed when users leave or change roles
- Are there any local accounts besides the administrator accounts
- If there is can you please provide the account names, last logon date, days required for password reset
- Is root access allowed in Linux systems.
- Is there local firewall enabled
- Are rules in place to limit control access to ports and services
- Is there a prelogin banner
- Are unused ports closed on the server
- Are your servers encrypted
- How often do you verify if an update requires the system to be restarted
- Is there a scheduled window to restart the servers to provide and update, can you provide evidence of the last restart.
- Do any of your machines contain sensitive/Mission critical data?
- Is antivirus/anti-Malware installed
- Are there any dual boot systems
- Do third party vendor have access to the server
- Are systems in place to ensure that all OS systems in a dual boot environment are updated.
- Is a host intrusion protection installed
- Is the KACE agent installed on the system

- Is there any logging software enabled on the server
- Are users able to browse webpages on the server

User Account Management

- Can you provide a list of all users with domain admin rights
- Is the administrator account for individual use with an academic or business need for this access.
- Student employees do not share local administrator password
- Student accounts do not have student employee-related access?
- Physical access grated by student IDs has a pre-populated termination date.
- Accounts are valid when the individual account holder has authorized access to the account or
  until the account is suspended by the University.
- Do all users take the FERPA and Information security training annually
- Do you monitor access to mailboxes and systems by unauthorized users

Applications

- Has default administrator password been changed to a password
- What are the password complexity rules applied to all account passwords
- Can you provide a list of users and their roles
- Are there any test account or service accounts for this application
- If yes, how many users have access to the service account / test account password.
- When was the last software patch applied?
- What is the latest version of the software
- Do you have a third party vendor access account
- Is there a process in place to ensure that only authorized licensed software is installed on the server
- Can you provide a list of all security related software and hardware systems

Physical Access

- Are all servers and desktops secured with security cables
- Has a location management software been installed and enabled on your computers
- Are all your machines kept in a room with a door that can be locked
- If applicable, is there a log of user access to rooms where confidential/sensitive information is stored on the server
- Is your inventory current with what is reported on the fixed access list
- Do you currently store confidential or sensitive data on a flash drive or external drive
- If yes, is the drive encrypted
- Are the drives kept in secure location
- Is there a defined process for equipment that must taken of campus by third party for repair