Information Security Checklist for Service Owners and System Administrators

The following questions should be used as a starting point to review information security related to the systems and services owned by each unit, department, or college. The service owner is responsible for addressing each of the items listed under the following topics areas. These topic areas are supported by the Standards and Guidelines associated with University Policy 311 Information Security.

System Acquisition, Development, and Maintenance

☐	Does the system integrate with the university's centrally managed authentication services?
☐	When considering the development of a new system or an enhancement to an existing information system, are you considering the information security requirements and discussing with ITS as appropriate?
☐	When considering the acquisition of a new system, are you carefully reviewing the security requirements and data protection language in the contract and discussing with ITS prior to purchase?
☐	When considering the acquisition of an application that involves credit/debit card payment transactions, have you included the University Controller's eCommerce Office for assurance of compliance with PCI-DSS and the university's Payment (Credit/Debit) Card Processing Standard?
☐	If using production data containing sensitive or confidential information for testing purposes, have you applied equivalent access controls and other securities to the test system as exist in the production environment?

Communications Security

☐	Before placing a system on the university network, do you ensure that it has been registered with ITS and has adequate security protocols installed and maintained to prohibit unauthorized access?
☐	Before allowing an outside vendor or other third party to connect a system to the university network, do you obtain prior review and approval from ITS?
☐	When transferring sensitive university information, have you ensured that agreements are in place between the university and the external party to appropriately protect the data?
☐	Before transferring sensitive university information, do you check the restrictions on how the data is to be handled which may be governed by: the guideline for data handling, a Data Security Plan, constraints placed by the Data Owner or the Data Security Officer, legal, regulatory or contractual restrictions, and/or export control regulations?

Access Control

☐	Are you using the university's centrally managed authentication services?
☐	Are you ensuring that accounts with elevated privileges adhere to the standard password requirements and are included in a documented audit conducted at least annually?
☐	Do you have a formal process for the authorization of user access?
☐	Is access granted to sensitive systems or data based on a need-to-know basis?
☐	Is access to systems terminated when an employee leaves or moves to another department?
☐	Are the access rights of all student workers and/or third party users removed upon termination of employment, contract or agreement?
☐	Do you have a formal process for reviewing user access rights at regular intervals?
☐	Are you requiring unique user IDs?
☐	If the business need requires the use of shared user IDs, is there a process in place and followed to change the password frequently and at a minimum whenever a member of the group leaves or changes jobs?

☐	Have you removed or disabled unnecessary vendor-supplied default accounts?
☐	For required vendor accounts, have you changed the default password following the installation of systems or software?

Data Management

☐	Have you identified the data classification level for information stored or transmitted to/from the system or application using the data classification standard?
☐	Have you ensured that the data is being handled appropriately according to its classification as outlined in the guideline for data handling?
☐	Have you obtained review and approval from the University CIO prior to securing a contract with a cloud service provider?
☐	When considering the transfer or surplus of hardware and/or media, have you ensured that data has been properly removed by destroying, purging, or clearing based on the guideline for hardware and media disposal?

Operations Security

☐	Have you implemented and do you follow a formal change management process?
☐	Have you implemented capacity management planning?
☐	Do you keep production, test, and development environments separate?
☐	Have you implemented controls to detect, prevent, and recover from malware?
☐	Have you ensured that backup copies of information, software, and system images are created and do you test them periodically?
☐	Do you maintain event logs and review them as appropriate?
☐	Do you maintain logs of privileged account holders' activity and review as appropriate?
☐	Do you review the vulnerability management scans for your system or application and determine the appropriate measures needed to address the related risks?

Physical and Environmental Security

☐	Are all servers kept in a secure area using appropriate entry controls to ensure only authorized personnel are allowed access?
☐	Do you periodically review the access lists and remove access for those individuals who no longer need it?

Vendors and External Parties

☐	When providing vendors and other external parties with the ability to access university information, do you document each party's rules for acceptable use and responsibility for implementing and managing access control?
☐	Do you obtain the vendor's or external party's documented commitment to employ industry best practices for the protection of sensitive university information?
☐	Have you stipulated the details for handling data upon termination of the contract or agreement?