UNIVERSITY OF
GEORGIA
Internal Auditing Division

240 S. Hull St. | Athens, GA 30602
706.542.1494|audit.uga.edu

INFORMATION SECURITY SURVEY

Unit: **Date:** **Prepared By:**

INFORMATION TECHNOLOGY

A. Information Technology Staff

1. How many of IT staff are employed full-time/part-time?
2. Does each IT staff member have a current job description?
3. Do job descriptions and evaluations include IT security duties?
4. Does the department have sufficient documentation to ease the transition of incoming/outgoing staff?
5. Does the enterprise have a privacy policy?
6. Is all staff aware of privacy considerations?
7. Are management/department users aware of the types of (private/nonpublic) information available to systems administrators?
8. Does the enterprise have a privacy policy to address this privileged information (confidentiality, agreement/nondisclosure agreement)?
9. Is the list of appointed information security contacts (DNLs) maintained by Infosec accurate and up-to-date for the department?
10. Are appointed DNLs aware of their roles and responsibilities?

B. Environmental / Inventory - Establish and maintain an inventory

1. What types of data are maintained by the enterprise (i.e., financial, statistical, graphical)?
2. In what form are they maintained (i.e., spreadsheets, databases, etc.)?
3. Is there any critical or confidential information maintained or handled? If so, how is it protected?
4. Are there any specific requirements for handling data (legal or regulatory requirements?)
5. Have you identified machines that store or require access to confidential information?
6. What type of operating systems exists?
7. Do you have an up-to-date network diagram?
8. How many workstations/servers, and mobile devices exist?
9. In how many locations is there IT infrastructure?
10. Has the wireless infrastructure been deployed? How is it secured?
11. Is staff instructed on how to lock workstations when they step away?
12. Are users aware that unexpected e-mail attachments should not be opened?
13. Is staff aware that many compromises are due to social engineering, compromised passwords, scam and phishing emails, and the sharing confidential information?
14. Does the enterprise have a network diagram that includes IP addresses, room numbers and responsible parties?

15. Are sensitive and critical devices reported annually in the USG Critical Systems Inventory?
16. Has the enterprise limited and secured physical and remote access to network services?
17. Is organization hardware upgraded at regular intervals?
18. Does the organization have a current documented inventory of hardware and software?
19. Is all organization software licensed?
20. Are IT purchases (equipment, software, and services) reviewed and approved by an appropriate part of the organization with an oversight role (governance/steering committee, Infosec and VP for IT, etc.)
21. Is license documentation available (licenses, purchase orders) if a software audit is required?
22. Does the enterprise have a firewall or IDS, or other software for network diagnosis? Does the enterprise have tools requiring privileges and access to confidential information acquired via routers, switches, IDS, and firewalls?

C. Antivirus - Install antivirus software with automatic updating

1. Does the enterprise have an antivirus policy?
2. Are all workstations running the latest version of antivirus software, scanning engine and virus signature file?
3. Are antivirus definition files downloaded automatically or manually? If manually, how often and why?
4. Does staff know who to contact when a virus is found?
5. Does organization utilize centrally-operated anti-virus software or provide equivalent detection and response capability (e.g. alerting, ransomware lockdown, etc.)

D. Passwords and other authenticators - Recognize the importance of strong authentication

1. Is there an organizational policy requiring strong passwords?
2. Is the enterprise using software that enforces strong passwords?
3. Is password caching disabled on domain member workstations?
4. Are passwords changed? If so, how often?
5. Are employees aware that passwords are not to be shared?
6. Is multi-factor authentication used for:
    a. all remote and / or administrative access to systems;
    b. all access to restricted data types;
    c. all access to 3rd party managed systems (e.g. cloud-based SaaS applications)?

E. Patching - Make it automatic-less work for you, less chance for compromise

1. Are software patches applied to all operating systems automatically when possible? If done manually, what is the release schedule?
2. Are patches applied to web browsers and third party applications? If yes, how frequently?
3. Does your team backup each machine before applying a patch?
4. Do you manage patches as part of change management process and test patches prior to applying?
5. Does the department have a documented process for patching?
6. Do you monitor vendor security advisories to be aware of patches to all relevant hardware and software?
7. Do you have a procedure for emergency patching?

F. Minimizing Services Offered by Systems - Eliminate unnecessary services reducing security risk and saving time in the long run

1. Have you identified services that each user needs to accomplish job assignments?
2. Have you removed unnecessary services which were installed by default?
3. Does the technical staff review security settings and policies?
4. Have you identified what services your systems are offering?
5. Have you taken security measures for remote access?

6. Are you using encrypted protocols for all services?

G. Addressing Vulnerabilities / Auditing – Eliminate many vulnerabilities with good system administration

1. Have you resolved vulnerabilities discovered by enterprise-wide scans?
2. Who is the contact for vulnerability scans?
3. Does the IT staff complete an independent vulnerability scan for the enterprise?
4. Has the enterprise deployed any form of firewalls or IDS (host or network based)? Any under consideration?

H. Backup and Recovery / Business Continuity - Allow easy recovery from user mistakes and hardware failure with backups

1. Are files regularly backed up?
2. Are files kept onsite in a secure location?
3. Are backup files sent offsite to a physically secure location?
4. Are backup files periodically restored as a test to verify whether they are available alternative?
5. Can you ensure that any forms of media containing confidential and sensitive information are sanitized before disposal?
6. Is there redundant hardware to allow work to continue in the event of a single hardware failure? Does the enterprise have the ability to continue to function if central services are not available?
7. Does the enterprise have the ability to continue to function in the event of a wide area network failure?
8. Have you responded to and recovered from any abuse issues / incidents?
9. Can critical systems be recovered if writeable versions of backups are encrypted by ransomware?