6. Computer Use: Employees must use only UA System Office-owned or approved laptops or devices for performing work-related tasks while working remotely. Personal computers should not be used to conduct UA System Office business to ensure data security and compliance. Employees are required to use appropriate campus VPN services when working from public, airport, hotel, or conference Wi-Fi networks, and it is recommended when not connected to a secure campus network (EDUROAM). Employees should protect UA System Office-owned or approved laptops from theft and unauthorized physical access, and should not leave them unattended in a public area, such as a car, restaurant, airport, etc. All UA System-owned computers must be encrypted and require a security key to start up the computer and must have authentication to log in. If your UA System Office-owned computer is lost or stolen, please contact a member of the UA System Office IT team immediately and submit an Incident Response Form.

7. Safeguarding Confidential Information: Employees must safeguard all confidential UA System Office information used or accessed while performing their job duties, regardless of their work location.

8. Remote Work Request and Agreement: A Remote Work Request and Agreement is required for an approved remote work arrangement. The employee:

    a. must sign a Remote Work Request and Agreement;

    b. agree to continue to meet the same performance expectations and the UA System Office's Standards of Behavior; and

    c. must maintain work hours, duties, and responsibilities consistent with their role.

9. A Remote Work Request and Agreement shall be subject to review at any time, but no less than on an annual basis as part of the employee's annual performance evaluation. An earlier review may be necessary when there are organizational or supervisory changes, or employee conduct and/or performance issues. Upon review, if it is

Employee Handbook Section 2 – See 2.2 standards of behavior
UA System Incident Response Form
Employee Handbook Section 6 – See 6.3 Responsible use of electronic resources