Purpose

The purpose of this document is to help managers and employees ensure the safety and confidentiality of Emory data and systems by adhering to sound computing practices and Emory’s information security requirements for telecommuting arrangements. This document identifies the security requirements and the parties responsible for implementation and/or ongoing adherence to those requirements. This document also contains a Telecommuting Security Agreement that must be used by managers to obtain written agreement from telecommuters to abide by the requirements specified in this document.

Administrative Requirements

It is the responsibility of school and business unit leadership (e.g. deans, department chairs, managers, supervisors) to ensure adherence with the following requirements for all individuals within the school or business unit who participate in telecommuting arrangements.

General Requirements

- All telecommuting arrangements must be approved and documented by the user’s manager or unit leadership.
- Only institutionally owned and supported computers that meet the requirements specified within this standard may be used for telecommuting arrangements.
- All users must sign the Telecommuting Security Agreement before being approved for telecommuting arrangements. These agreements must be kept on file by the telecommuter’s manager or unit leadership.

Technical Requirements

It is the responsibility of school and business unit IT leadership to ensure adherence with the following requirements for all individuals within the school or business who participate in telecommuting arrangements.

Standard Build Requirements

- Systems issued to users under telecommuting arrangements must be supported by unit level IT personnel and actively maintained in accordance with locally defined configuration standards that addresses common security considerations such as: security patches, anti-virus, removal of administrative rights, authentication, auditing, disabling unnecessary services, password complexity, user privileges, local security policies, etc.

Security Update Requirements

- All systems used to telecommute must be kept up-to-date with the most current security patches for the operating system as well as any applications such as Anti-virus software, Microsoft Office, Internet Explorer, Firefox, etc.
- Only operating systems and applications currently supported by the vendors are allowed. Software that is no longer supported with security updates are prohibited (e.g. Windows 98, Windows 2000).
- The system should be configured to automatically retrieve and apply security updates at least weekly.
- Active management of systems used to telecommute via LANDesk is highly encouraged.

Anti-Virus Requirements

- All systems used to telecommute must have anti-virus software installed and properly configured.
The anti-virus software must be kept up-to-date with the most current anti-virus pattern files (sometimes called anti-virus signatures) and scan engines, and be configured to automatically retrieve and apply updates to anti-virus pattern files and scan engines on a daily basis.

The anti-virus software must be configured to scan files in real-time (sometimes called active mode).

The anti-virus software must be configured to scan the entire system (all hard drives) at least weekly.

The anti-virus software must be configured to alert upon the discovery of a virus.

The anti-virus software should be configured to first clean infected files, and then quarantine the virus infected files if the clean is unsuccessful.

**Network Security Requirements**

- All systems used to telecommute must be protected with a firewall.
- The firewall may be either hardware or software based.
- The firewall must be configured to block all unsolicited inbound connections.

**Authentication/Authorization Requirements**

- All systems used to telecommute must require users to login before using the system.
- Administrative rights should be restricted to local IT staff. Telecommuters should not be given administrative authority to the computer used for telecommuting.

**Security Incident Reporting Requirements**

- If a system used to telecommute is lost, stolen, compromised, or suspected of being compromised, the user must immediately report the incident to their manager and local IT support. Local IT support is responsible for reporting the incident to the central IT security department for their institution (University or Healthcare)

**User Requirements**

It is the responsibility of individuals who participate in telecommuting arrangements to ensure their adherence with the following requirements.

**General Security Requirements**

- Users must not attempt to bypass security measures or modify security configuration settings.

**Network Security Requirements**

- Only the following network connectivity methods may be utilized for telecommuting arrangements:
  - Connect to a wired network and utilize the Emory VPN.
  - Connect to an Emory owned and managed wireless network utilizing built-in VPN technology. Home wireless networks may not be utilized for telecommuting. The use of home wireless networks solely for accessing email and public web sites may be allowed if authorized by unit management.
    - Note: Emory is researching a solution that may allow business units to lease and deploy Emory owned and managed Aruba wireless access points to telecommuters' homes.

**Authentication Requirements**

- Passwords for all accounts on the system must meet the minimum complexity requirements defined by their institution
  - Emory University
    - Passwords must be between 6 and 30 characters long.
    - Passwords must not be your NetID, your name, or a word found in a dictionary.
  - Emory Healthcare
    - Passwords must be between 6 and 8 characters long.
    - Passwords must not be easily guessable or words found in a dictionary.

**Data Protection Requirements**

- Sensitive data includes but is not limited to: Social Security Numbers, Government issued ID numbers (e.g. Driver’s license number), financial account numbers (e.g. bank accounts, credit card accounts),
data protected under HIPAA (e.g. patient information), data protected under FERPA (e.g. student grades), and data entrusted to Emory by governmental entities (e.g. Veterans Administration, NIH) or other parties on the condition that the data be adequately protected.

- Users must not store sensitive information on any system used for telecommuting unless authorized to do so by their manager. Sensitive information should not be stored on any systems used for telecommuting unless absolutely necessary, and only the absolute minimum necessary information required to perform the job should be stored. Network file storage solutions should be utilized instead, whenever possible.
- Sensitive data should be encrypted if possible using the native capabilities of the application used to create the data (Excel, Word, Acrobat, etc.). Unencrypted files containing sensitive data should be password protected if possible.
  Note: Users who store sensitive data on systems used to telecommute may be required to encrypt their system with Full Disk Encryption (FDE) once an enterprise FDE solution has been selected.
- Users must never allow unauthorized individuals to access sensitive data or use the system issued to them for the telecommuting arrangement.
- Users must not store sensitive data on non-Emory owned systems or removable media (CD’s, USB hard drives, flash drives, etc.).
- Stored data that is no longer needed must be promptly deleted from the system. Sensitive data must also be deleted from the system when the telecommuting arrangement terminates or the user is requested to do so by their manager.
- Any system or removable media used to store sensitive data must be disposed of in a manner that renders any sensitive data on the device/media unrecoverable. Examples include physical shredding, logical disk wiping, and degaussing.

Physical Protection Requirements
- Laptops should be physically secured to an immovable object with a cable lock anytime they are unattended in an area that is not physically secure (e.g. hotel rooms, conference rooms). Never leave a laptop unattended in a vehicle.

Security Incident Reporting Requirements
- If a system used to telecommute is lost, stolen, compromised, or suspected of being compromised, the user must immediately report the incident to their manager and local IT support.
- Any system used to telecommute must be made available upon request by IT Security for examination in order to respond to actual or suspected security incidents.

Compliance Requirements
- Users who access sensitive information that is protected by regulation (e.g. HIPAA, FERPA) or contract (e.g. credit card data) must comply with any additional requirements dictated by the governing regulations/contracts.

Sanctions
Failure to comply with the requirements specified in this document may result in disciplinary action, up to and including termination of employment and/or termination.
Telecommuting Security Agreement

User’s Name: __________________________
User’s Title: __________________________
User’s NetID: __________________________
User’s Manager: __________________________
Manager’s NetID: __________________________
Authorization Begins: __________________________
Authorization Expires: __________________________

I have read and understood the “Information Security Requirements for Telecommuting Arrangements” document and agree to abide by the requirements specified within the document. Additionally, I understand that failure to comply with the requirements specified within this document may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

User Signature: __________________________ Date: __________________________

User is authorized to use a home wireless network solely for the purpose of accessing email and public web sites: Yes  No (circle one)

User is authorized to store sensitive data on the Emory owned system issued to the user for the telecommuting arrangement: Yes  No (circle one)

If Yes, specify which sensitive data (or data types) the user is allowed to store on the system:
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________

Manager Signature: __________________________ Date: __________________________