Device and Information Security Acknowledgement Form

This form has been created to assist ECE faculty and students meet University requirements for network security and use of information technology resources. The form is to be filled out by the primary administrator/user of each UT owned device, or any device connected to the University wired network. This is to include devices with a variety of operating systems, with the exception of mobile operating systems such as iOS, Android, BlackBerry, Windows Mobile/RT, for example.

Device Covered *
- Laptop
- Desktop
- Server Appliance
- Tablet/Slate
- Other (e.g., networked storage)

If Other, Please Explain

Manufacturer *

MAC Address *
How to Find the MAC Address

2nd MAC Address (if applicable)

3rd MAC Address (if applicable)

Operating System *
Pleas enter the Operating System information including the version number, ex. Mac OSX 10.8.2, Windows 8.13

Ownership of Device *
- UT-owned
- Personally-owned

If UT-owned, Provide the UT Inventory Tag ID *
Device Administration

UT EID of primary administrator/user *

UT EID of ECE Faculty Member who is the point of contact for this device. (For non-UT systems on the wired network, please list your faculty supervisor) *

Logon Authentication *
UT Austin Domain (device bound to Austin AD & EID credentials are used to authenticate)
Local Account (accounts manually created locally on the system)
Third-party Authentication (e.g. Microsoft account, Fingerprint, pre-boot logon)
None (e.g. automatic login)

For Third-party Authentication, Indicate Source of Authentication

Type of Encryption Used on this Device *
Self-encrypting Disk
Bitlocker
FileVault
SecureDoc
TrueCrypt
LUKS
Other
None
Check more than one if you use a dual-boot system. Learn more about encryption

If Other, please list

Maximum Data Sensitivity That May Be Accessed or Stored on This Device *
UT Category 1 (e.g. HIPAA, FERPA, SSN, sensitive research) Extended List of Category-1 Data Examples
UT Category 2 (e.g. contents of specific e-mail, salary, date of birth) Category 2 Definition
UT Category 3 (e.g. publicly available) Category 3 Definition
Learn more on Data Classification definitions

Information Security Certification

I understand that information that is created by my UT activities or that may be accessed by me while performing my UT responsibilities may be sensitive and must be protected as required by the Information Resources Use and Security Policy and operational implementation of the UT System Information Resources Use and Security Policy (UTS-165), with additional requirements as are defined by The University of Texas Information Security Office
To the extent of my administrative control, I agree to protect any and all known sensitive data that may be stored on this device as per the ECE-SUGSMC policy, and prevent the distribution of such data except to other approved devices or approved storage services.

I Agree

**How is the OS Configured to Apply Updates?**
- Install Automatically
- Download Automatically
- Check for automatically, but download and install manually
- Manual

[Guide for Windows] [Guide for OS X]

**What backup method is used for the documents and data on this device?**
- UTBackup/Crashplan
- UT Box
- Third-party Service (Dropbox, SkyDrive, GoogleDocs, Carbonite, etc)
- Manual Backup (external hard drive, USB thumbdrive, etc)
- None

**For third-party services, what service(s) is(are) used:**

**What anti-virus software is activated on the device?**
- System Center Endpoint Protection/Forefront
- Symantec/Norton
- McAfee
- ClamXav/ClamAv
- None
- Other

**If other, please list:**

**Does the primary login account have administrator privileges disabled?**
- Yes
- No

[How to Not Login as Administrator] [Guide for Windows] [Guide for OS X]

**Does the password for the primary user meet UT guidelines for strong passwords?**
- Yes
- No

[How to create a strong password]
Is the device configured to lock the console after 15 minutes or less of inactivity? *
Yes
No

Device configuration for inactivity

Is the device configured to require a password on resuming from suspend? *
Yes
No


Device and Network Security Certification

I understand all University and personal devices accessing the University wired network must be maintained in accordance with the operational UT System Information Resources Use and Security Policy (UTS-165), supplemented by the University of Texas at Austin Acceptable Use Policy, and additional requirements as are defined by The University of Texas Information Security Office. I certify that the device will be administered in accordance with these policies.

I Agree

Software Acceptable Use and Licensing Certification

As per section 5.24 of UT Austins Information Resources Use and Security Policy, "all software used on university computers will be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the university".

I understand that only properly licensed software may be used on university owned devices, or used for university business on personally owned devices, and that such software must be used in accord with the terms of use or license agreements of the software.

I Agree