

Protecting Data on Vulnerable Devices (Security Practices Bulletin #1)

Table of Contents

1. Introduction.....	1
2. Q&A	2
3. Revision History	3
4. Approvals.....	3

1. Introduction

Improvements in computing technology over the last few years mean that increasing amounts of data are being stored on smaller, handier devices, such as laptop computers, thumb drives, PDAs, and cell phones. Unfortunately, their portability makes these devices very easy to steal. Because of the rise in their use and the ease with which they can be lost, UT System is putting a high priority on the following practices:

- As much as possible, Category-I data will not be stored on portable devices.
- Category-I data will not be stored on any portable device or any device that faculty and staff use at home (whether personally or departmentally owned) without documented permission from the [data owner](#).
- Category-I data must be encrypted when it is stored on portable devices or any device that faculty and staff use off campus.

The practices are outlined in Security Practice Bulletin #1, [Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices](#).

For specific suggestions for protecting your portable device, please see [the ITS Web site](#).

These requirements require everyone to change their behavior and perhaps use new technology to protect their data. ITS is working with the ISO and university IT professionals to implement central solutions that will address a broad range of needs. We are also providing tips in this document that will help you immediately assess whether you need to store Category-I data on your devices and how to secure it if you do.

Protecting Data on Vulnerable Devices (Security Practices Bulletin #1)

Document Version: Approved

If you have any questions about securing your data or you are concerned that data may be at risk, please do not hesitate to contact the [Information Security Office](#).

2. Q&A

2.1. What is a Security Practice Bulletin?

Security Practice Bulletins allow UT System to address gaps in policies quickly to address immediate problems. [UTS-165](#) did not address portable devices or devices that faculty and staff use to work at home.

2.2. To whom does the standard apply?

All faculty and staff at The University of Texas at Austin. This includes graduate students with staff titles such as Research Associate or Teaching Associate.

2.3. To what computing devices does it apply?

- Any portable device, including, but not limited to laptops, PDAs, USB drives (thumb drive), portable media.
- Any home computer that you use to work on or store Category-I data.
- Any university-owned desktop or other device that you have checked out for use off campus.

2.4. Under what authority is this standard issued?

UT System has issued this as an extension of UTS-165, the policy that governs the use of information resources at the university. UTS-165 has been adopted for UT Austin as the [Information Resources and Use Security Policy](#). It will soon be incorporated into the Handbook of Operating Procedures.

2.5. Why is this so important?

Faculty and staff are storing sensitive digital data (Category-I data) on devices that are easily lost or stolen because they are so portable. This is an immediate risk that must be mitigated. When sensitive digital data is lost or stolen, it costs the university thousands of dollars *per person whose data is exposed*. In addition, the university can suffer loss of reputation, which can translate to lost donations and prestige. Finally, there is the real cost to you in terms of lost work and research data.

2.6. What are the consequences for not complying?

Your job is at risk if you do not comply with the requirements and you lose a portable device that has sensitive digital data, or if your home computer is stolen and it has sensitive digital data on it.

3. Revision History

Version	Date	New	Original
Protecting Data on Vulnerable Devices (Security Practices Bulletin #1)	3/4/2011	Converted web page to PDF	No changes

4. Approvals

Name	Role	Members	Date
Chief Information Security Officer	Approval	Cam Beasley	3/7/2011