

Storing Data on Mobile Devices

The basis for securing data on mobile devices is from the State Information Services Board (ISB) Policy NO. 401-S4, Information Technology Security Standards, Securing Information Technology Assets

Section 4.1 on Data Security and section and Section and Section 5.8 Mobile Computing are relevant. Details from these sections are below. Note that section 4.1. 2 classifies personal information which is not “public” at Category 3 and that agencies must “Encrypt Category 3 data or above on mobile devices using industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST)” **If** the agency have approved and document the use of category 3 data or above on mobile devices. Seattle Central and the Seattle District have not filed any approval for such use and do not plan to do so. Even if such approval were on file, we would be in violation of the standard if the data were not encrypted.

Seattle Central Community College IT Services strongly recommends storing sensitive or confidential data only on our secure Citrix servers. While storage on a local (non-mobile) desktop is allowed, it is less secure.

Excerpts from sections 4.1 and 5.8 of the ISB Standard:

4.1 Data Classification

4.1.1 Agencies must classify data into categories based on the sensitivity of the data.

4.1.2 Agency data classifications must translate to or include the following classification categories:

- (1) Category 1 – Public Information
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.
- (2) Category 2 – Sensitive Information
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.
- (3) Category 3 – Confidential Information
Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:
 - a. Personal information about individuals, regardless of how that information is obtained.
 - b. Information concerning employee personnel records.
 - c. Information regarding IT infrastructure and security of computer and telecommunications systems.
- (4) Category 4 – Confidential Information Requiring Special Handling
Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:
 - a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
 - b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

5. 8 Mobile Computing

Examples of mobile devices include laptops, smart phones, Personal Digital Assistants (PDAs), accessible equipment, and portable data storage devices such as tape drives, zip drives, removable hard drives, and USB data storage devices.

Agencies must implement policies and procedures controlling the use of Category 3 and above data on mobile devices. At a minimum, agencies must

- (1) Approve and document the use of category 3 data or above on mobile devices.
- (2) Encrypt Category 3 data or above on mobile devices using industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST).
- (3) Implement policies and procedures that address the use of portable data storage devices.