Storing PII Data and Device Requirements

What is Personal Identifiable Information (PII)?

- Social Security Number, payment card number, ethnicity information, disability information, veteran status, medical information, academic records, disciplinary information, employment performance information, password information.

What does ***Stores PII Data*** mean?

- There are 2 locations authorized for PII data storage.
    1. Secured network share assigned to your department from ITS
    2. Your local computer with the appropriate permission, signatures and security measures in place

All devices will have the following: (Automatic Operating System Updates and Patches, Automatic Antivirus Updates, MIR, DLP, & Password Authentication)

Risk Level	What you do with PII data	Signed PII Data Form	Local Device Security Measures Required
Low	Never access PII data	Not Required	
Medium	Access PII Data	Not Required	- Inactive Session Timeout
High	Access & Stores PII Data	Required	- Inactive Session timeout - Device Encryption - Local Administrator Rights Revoked - Approved Software only

* Data classifications and requirements are from the South Carolina Division Information Security Office and the University of South Carolina Information Security Office. For more information see the following documents (Data Classification Schema and Data Security Requirements)