**PURPOSE**

This electronic data security procedure explains methods to be used in the protection and storage of potentially sensitive electronic data. It is supplemental to and not a replacement for the University Policies related to data security.

**RESPONSIBILITY**

HPL associated faculty, staff and students with access to potentially sensitive electronic date are responsible for its security. Research investigators are responsible for managing security for data related to their studies.

**PRODUCT INFORMATION**

The HPL follows University product standards with regard to data security and supplements as needed where products are not defined. Primary storage for sensitive data will be on the HPL departmental Piratedrive provided by the University. Primary sources of data such as lab instrumentation will be password protected. Storage external to Pirate Drive and primary sources will be considered temporary and will require password protection and/or file or folder level encryption.

**IMPLEMENTATION**

The following procedures should be followed to secure HPL related potentially sensitive electronic data:...

1. Piratedrive - Primary storage for sensitive electronic data will be on the departmental pirate drive. The HPL Pirate Drive will be administered by the director and associate director of the Human Performance Lab. Research investigators will be assigned a folder for which they become the administrator of data security w/in their labs.
	1. Investigators will administer permissions w/in their folder to staff and students.
	2. Investigators may appoint a Technician, Post-Doctoral Student, PhD student or co-investigator to co-administer the security of their folder.
	3. Each investigator will keep an encryption password key document in their primary folder from which their lab staff will get the passwords used to encrypt data that leaves Piratedrive. The password will be changed every 4-6 months and the encryption password key document will journal those passwords.
	4. Each Investigator folder will have a Piratedrive Security Review Log. This log will be updated based on access permissions added, removed or changed by the investigator or co-administrator of the investigator’s folder.
2. Outside Piratedrive - Use and storage of sensitive data outside Piratedrive should be temporary and always encrypted. The computing device used should be password protected to prevent unauthorized use. The sensitive data file must be encrypted either through inherent capabilities of the software used, as in Excel, or via third party tools such as TrueCrypt or Zip utilities.
	1. Potentially sensitive data on flash drives or other forms of removable drives should be de-identified if feasible.
	2. Sensitive data not de-identified on flash drives or other forms of removable drives must be encrypted as indicated above and must be temporary on such devices.
3. Email - Emailing potentially sensitive data is prohibited unless the data is encrypted. Emails that include sensitive information should be sent using IronPort. This is a service that can be obtained through ECU IT and works with Outlook. Students will not have access to this service.
4. File sharing outside ECU – Tools for sharing files over a longer period of time with collaborators outside ECU are available by contacting ECU ITCS. The use of cloud file sharing services for ECU electronic information or sensitive electronic data is prohibited by ECU. These services include but are not limited to, iCloud, Google Docs, SkyDrive, DropBox…etc.
5. Departure of personnel - When a student, faculty or staff graduates or leaves the university, the study investigator or supervisor of that individual will request all sources of sensitive data belonging to the University or study. The PirateDrive access will be changed as appropriate by the investigator(s) and the change will be logged in the Piratedrive Security Review Log(s).
	1. Flash drives or other external storage devices purchased by the university should be returned and wiped by fully formatting the device before reuse or surplus. ECU IT should be contacted for current procedures.
	2. Computers belonging to the university should be returned. ECU IT should be contacted to wipe the computer hard drives before reuse or surplus.
6. Primary sources of data - Primary sources of data collection. All primary sources of data collection that include potentially sensitive information will be password protected. Data will remain on primary sources only as long as needed for the work being performed. If removed from primary sources any potentially sensitive data will be encrypted and placed on Piratedrive or follow bullets points #2 and #3.
	1. Primary sources of data should not be connected to the internet unless IT has approved the security protocols that are used to transmit data over the network.
	2. Primary sources of potentially sensitive data include but are not limited to…
		1. Metabolic Carts
		2. DXA System
		3. EKG System
		4. Pulmonary Function System
	3. Were possible, subjects should only be identified based on a subject ID and not by name on these primary sources of data.
7. Data collection services – Use of vendors for data collection services must be coordinated with the HIPAA Privacy Officer and ECU ITCS.

**ADDITIONAL PRECAUTION**

The Human Performance Lab encourages all faculty, staff and students to be mindful about data security. University policy on data security can be found on the ECU website along with approved tools to aid in data security.