Policy 1114: Appendix C
Procedures for Requesting Authorization to Store Highly Sensitive Data

There is a high risk of unauthorized disclosure of highly sensitive data when such data are stored, especially on mobile data storage devices and media. The university strictly limits the circumstances under which highly sensitive data may be stored on any storage device and media. All of the requirements that follow must be met when, due to a specific business need, highly sensitive data must be stored electronically.

Anyone needing to store highly sensitive data electronically must complete the Authorization to Store Highly Sensitive Data - Request Process at https://hsd.mesa.gmu.edu/ . A Chief Data Steward must approve the request. Permission, if granted, is for only one year and only on the device or media specified on the form.

Highly sensitive data must be encrypted if stored electronically, according to encryption methods recommended by the University's *Information Security Officer*. If the encryption program is not compatible with the device or medium, an approved mitigating control must be used.

The workflow is as follows:

1. The requestor completes the form, stating the need, the specific data, and the proposed storage device or media.
2. The requestor forwards the form to the appropriate department head or chair for approval.
3. If the department head approves, the department head forwards the form to the *Chief Data Steward*.
4. The *Chief Data Steward* approves or denies request.
5. The *Chief Data Steward* retains original and sends copies of the form to department head, IT Security Office and the requestor.
6. If permission is granted to store the highly sensitive data, the requestor contacts the ITU Support Center and requests encryption.