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,

- Set up a consultation at Highly Sensitive Data - Information Technology Services (gmu.edu) to have the use case evaluated.
- Obtain approval from the IT Security Office.
- Must encrypt such data 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 storage media, an approved mitigating control must be used.

The workflow is as follows:

1. The requestor completes the form at Highly Sensitive Data - Information Technology Services (gmu.edu), stating the need, the specific data, and the proposed storage device or media.
2. IT Security Office receives and reviews the form, works with the department head and Chief Data Steward to evaluate and consider the request for approval.
3. If permission is granted to store the highly sensitive data, the requestor contacts the IT Service (ITS) via Team Dynamix ticket to request onboarding with the required controls including encryption.