Policy 1114: APPENDIX A

Protected Data Types

Data types on this list will be subject to high levels of security precautions, including a requirement that the data classified as 'Protected Data - Highly Sensitive' be encrypted when stored and during transmission. This list is not intended to contain all protected data types, just those that have the potential to cause significant damage to individuals or the university.

Two classes of Protected Data have been identified, as follows:

I. Protected Data - Highly Sensitive

Data that:

1) by their personal nature can lead to identity theft or exposure of personal health information, or
2) a researcher, funding agency or other research partner has identified as highly sensitive or otherwise requiring a high level of security protection. No one is permitted to store this data unless:
   a. Due approval is obtained from the IT Security Office. Approval requests can be submitted using the process and form published at its.gmu.edu/service/highly-sensitive-data.
   b. The storage device or media are protected using approved methods and levels of encryption.

      i. With respect to the potential for identity theft, the following information has been defined by the university as highly sensitive:

      - Student Information
      - Social Security number associated with a personal identifier
      - Date of birth associated with a personal identifier
      - Driver's license information associated with a personal identifier
      - Visa information
      - Employee/Donor/Contractor/Affiliate Information
      - Social Security number associated with a personal identifier
      - Date of birth associated with a personal identifier
      - Driver's license associated with a personal identifier
      - Background checks

      ii. With respect to technology related information and systems, the following information has been defined by the University as highly sensitive:

      - Passwords/PINs and cryptographic private keys associated with User IDs
      - Network diagrams that include detailed configuration information or network device associated with systems categorized as 'High-Risk'

- configurations (including server names, IP addresses, etc.)
- Security configurations related to network devices and systems, etc.

iii. With respect to financial data, the following information has been defined by the University as Highly Sensitive:

- Credit card numbers associated with a personal identifier
- Financial aid/scholarship information that is defined by the U.S. Department of Education as requiring a high level of security protection, including student and parent tax returns
- Bank account information associated with a personal identifier sufficient to provide access to the
- account

II. Protected Data – Restricted

Data that by their very nature or regulation, are private or confidential and must not to be disclosed except to a previously defined set of authorized users. Examples include:

- Data defined as confidential by the Family Educational Rights and Privacy Act (FERPA)*
- Employee performance evaluations
- Confidential donor information,
- Some research data
- Minutes from confidential meetings
- Accusations of misconduct, or any other information that has been identified by the University, its contractors or funding agencies, or Federal or State regulations, as private or confidential and not to be disclosed.

*With respect to FERPA data, please consult the Registrar's web site for the complete list of restricted data types: http://registrar.gmu.edu/ferpa/