Sensitive Data

Personally Identifying Information (PII)

Virginia Tech’s Policy for Protecting University Information in Digital Form (Policy 7105) defines Sensitive information as: all university information that could cause physical, financial, or reputational harm to the university or to members of the university community if released inappropriately. Further, Policy 7105 defines Digital Form as the technology of computers and data communications, and includes products of those systems, including printed reports.

Per the IT Security Office, PII Data includes:

- Social security number
- Bank account numbers
- Driver’s license numbers
- Credit card numbers
- Debit card numbers
- Passport numbers

PII information should not be stored on any users device (laptop, desktop, mobile device, tablet) in an unencrypted state. The best rule is to delete this data. If there are business reasons for retaining the data, it must be stored in an encrypted state. If this data is to be shared for business purposes, whether that sharing takes place through the shared folders or via email, it must be in an encrypted state. Contact your Departmental IT support person, your Area Information Technologist, or the Ag Help Desk (aghelpt@vt.edu, 540-231-4865) for more information on available encryption options. Please review the Standard for Storing and Transmitting Personally Identifying Information document from the VT IT Security office.

Payment Card Industry Data Security Standard Council (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security requirements developed by credit card companies to ensure consistent security measures for sensitive credit card holder data. The purpose of protecting this data is to protect customers from identity theft and/or compromise of their credit or debit card or any financial data related to a credit or debit card.

The following should never be kept in any form:

- Primary Account Number (PAN) - 14 or 16 digit numeric code located on the front of a credit or debit card
- Cardholder Name
- Expiration Date
- Service Code - The three digit code on the back of a credit or debit card
If PCI Data is found in any form is should be deleted immediately. For more information, visit: http://www.policies.vt.edu/3610.pdf.

Family Educational Rights and Privacy Act of 1974 (FERPA)

FERPA is also known as the Buckley Amendment. The intent of the Act is to protect the rights of students and to insure the privacy and accuracy of education records. The Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. Students who are or have been “in attendance” at the institution, regardless of instructional delivery, age or status in regard to parental dependency are protected by FERPA. Disclosing Personally Identifiable Information along with information specific to the Student’s educational record is not allowable without consent or legitimate educational interest.

Per the Office of the Registrar, the University’s interpretation of FERPA PII includes but is not limited to:

- The student’s name;
- The name of a student’s parent or other family member;
- The address of the student or student’s family member;
- A personal identifier such as the student’s social security number or student identification number; includes partial numbers
- A list of personal characteristics that would make the student’s identity easily traceable; or
- Other information that would make the student’s identity easily traceable.

While there is no encryption requirement mandated in Virginia Tech’s policies on protection of FERPA data, there are strict guidelines relating to the electronic transmission of this data. Email standards for FERPA data are as follows:

- Do not include personally identifiable data in totality: full student ID number and full name
- Do not list name and ID number in subject line
- Communicate using either: 999999999 (ANW) or Alice N. Wonderland (x9999) or 999999999(Wonderland).
- Do not attach spreadsheets or scanned documents with full identifiers or non directory info via email; communicate spreadsheets via secure links

Best practice is to delete this data from your computer or mobile device if there is no further business need. For more information, visit: http://www.registrar.vt.edu/privacy/index.html.