Data and Personally Identifiable Information Security Policy

Definitions

Sensitive Information is defined as any information that provides personally identifiable information (PII) on a student, faculty or staff member. PII is information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual. This includes, but is not limited to, information such as social security number, date and place of birth, mother's maiden name.

Portable Mass Storage Device is defined as any device which is capable of transporting digital files outside the internal storage device of a Roane State computer or network. They include such devices as floppy disks, CD/DVD's, flash drives, zip drives or external hard drives.

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

Procedures

General

Access to data residing in administrative systems and applications at the institution is to be granted only to those individuals who must, in the course of exercising their responsibilities, use the specific information. Data Custodians are responsible for granting access to the information.

The copying, downloading, FTP transfer or otherwise duplicating PII data on a computer, website, floppy diskette, CD/DVD, tape, USB device, or other such mobile storage device for purposes other than backup by authorized personnel is prohibited.

All paper files containing PPI including academic records and payment record must be kept in a locked file cabinet, except when the file is currently being worked on.

Control of Sensitive Information

Under no circumstance should sensitive or confidential information be transferred to or stored on any personally-owned laptops, removable media, or home computers. One may access administrative

systems and work with sensitive or confidential information from college-owned computing devices, but may not make a copy of that information and store it locally on the device. Any file containing personally identifiable information must be stored on the individual's "U" drive on the network.

Unsecure laptops or removable storage devices will not be used to transport or store sensitive information should a requirement exist for sensitive or confidential information to be stored on a laptop or removable media, the device must be encrypted and be physically secured when unattended. Unless written permission, as outlined above, has been granted, removable media such as USB drives or optical disks (e.g., CD-ROM or DVD-ROM) should not be used to transport sensitive or confidential information.

Laptop users are responsible for securing laptops at all times, but especially when traveling. (See Securing Laptops below.)

Email Transfer of PII

Email should not be used to transmit PII, when ppi have to be emailed. The user has to encrypt the file (PDF, WORD, EXCEL) with a password.

Security of Laptop

Laptops must be secured in a locked office when unattended for an extended length of time or left overnight.

When laptops are taken out of the office, the laptop must be kept under positive control of the owner. It should be in hand, in sight or locked in a secure location at all times.

Computers should be log off at the end of the day.

Lock your computer wherever you your desk, to prevent un-authorized access.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.