Sensitive Data Protection Best Practices

Sensitive Data

Data, regardless of its physical form or characteristics, with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security related data. It also includes data that is not open to public examination because it contains information which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the college or compromise public activities. Examples include: passwords, intellectual property, ongoing legal investigations, medical or grades information protected by FERPA or HIPAA, social security numbers, birth dates, professional research, student work, bank or credit card account numbers, income and credit history.

Data Handling Guidelines:

- Do not collect and/or store SSN unless it is required by a federal or state agency and there is no other option in terms of unique identifier. If collection and storage of SSN are required for operations in a given unit, register this by notifying the Office of Budget & Compliance explaining why SSN must be utilized and how and where it is being collected/stored.

- Use the CCM ID assigned to all individuals as the unique identifier for all CCM entities. If CCM ID is not available or does not exist for certain populations, use a non-SSN type of ID.

- Data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on central administrative systems only.

- Avoid storing data on departmental servers or creating “Silo” databases that duplicate data on central administrative systems.

- Inventory and identify the data under your control that is external to central administrative systems. Know where you have data and in what form (electronic, paper, etc.). Purge or delete data files in a timely manner. That is, keep data you control “cleaned up”. Data on old machines, network drives, backup tapes, etc. should be inventoried and purged/archived or moved to more secure locations. If the data are considered an official college record they are to be preserved until their official retention period has been met and only purged or deleted after approval from the Records Management Department.

- Do not store on or copy sensitive data to mobile, external storage devices such as CD, DVD, laptops, USB memory keys, PDAs, cell phones, or any other device that can easily be stolen or compromised.

- Do not store on or copy sensitive data to local workstations or network drives unless such data is not available on centralized systems. If you must store data on workstations or network drives, it is your responsibility to secure your workstation and/or ensure that only authorized individuals have access.

- Do not use shared network drives to share or exchange data internally or externally unless you are certain that access to those shared drive resources is restricted to individuals authorized to handle such data. Example: Do not put anything sensitive or confidential on what is currently the F:/ shared drive in a common folder. Potentially, everyone with a network account can access it.

- Know and understand your environment technically. Understand who has access to areas you send, receive, store, or transmit data. Attend any CCM Sensitive Data Protection course offerings.

- Transmission of any sensitive data should be encrypted. Websites should use HTTPS or SSL encryption if they collect data. FTP/Telnet or any other means of transferring files and data should use encrypted versions of these protocols: Example SSH and SFTP. When in doubt, contact the Technology Help Desk.

- Do not send, receive, or store any sensitive data using email under any circumstances. Email is not secure.

- Under no circumstances should credit card numbers be collected and stored on standalone devices, digital media, or paper media. Processing credit card numbers should be done via secure methods which authorize or deny the transaction in real time but DO NOT retain or store the credit card number. Collecting credit card numbers via phone calls, websites or email and retaining such numbers on paper or in electronic files for some sort of periodic processing is bad practice, insecure and should be discontinued immediately. If you need help processing credit cards securely, contact the Technology Help Desk.

- Report any breaches, compromises, or unauthorized/unexplained access of sensitive data immediately by contacting the Office of Budget & Compliance.   For more detail on the proper notification procedure, click here.