Data Sensitivity Classification Policy FAQ

Last Updated 11/13/2024

Why Is This Policy Important?

- What is the goal of applying data sensitivity levels to data and documents?

  The goal is to equip those who are working with these types of data and documents with a standardized measure of sensitivity to better guide proper storage and distribution and reduce the risk of improper disclosure of confidential or sensitive information.

  The DSC Policy will promote Berry's responsible use of data in three ways:
  Effectiveness: Improving our ability to effectively leverage data.
  Security: Protecting Berry's data from exploitation by bad actors.
  Privacy: Honoring Berry's commitment to safeguard data from unauthorized or unwarranted disclosure.

- What are the risks if we do not apply data sensitivity levels?

  Accidental disclosure of confidential or sensitive information.
  Exploitation of data by bad actors who obtain illicit access to data.
  Lack of clarity and confidence regarding how data may be stored and used.
  Violations of student privacy.
  Reputational risk to the institution.

- What happens if I ignore this policy?

  Policies such as this one are designed to protect students, individual employees, and the institution at large. Ignoring this policy increases risks of accidental disclosure of data that may put at risk the privacy of students, faculty, or staff.

Understanding Data Sensitivity Levels

- How do I know the level of sensitivity for a document / data?

  All documents within the Microsoft Ecosystem will have the option to add a Sensitivity Label at the point of saving the document. The labels are color-coded for easy reference.

- I have a document without a defined sensitivity level; am I responsible for defining one?

  Yes; for data and documents that you work with, you should select the appropriate data sensitivity level.

  If you're working with data beyond your immediate area of responsibility, work with the data steward to determine the appropriate data sensitivity level. In general, the sensitivity level of a document should be as high as the most-sensitive data contained within.

- If I share data responsibly with my staff who have a legitimate use for this data and then they do something irresponsible with it, am I at fault?

  If you follow the procedures for the appropriate level of sensitivity, including storage and transmission guidelines, then you are not responsible for others' errors.

- As a supervisor, how do I ensure that my staff understands and complies with this policy?

  Opportunities for training will be provided, as will basic guidelines such as this document. It's important to take time to meet with staff and discuss the importance of these ratings as well as the proper ways to store and share documents and data.

Use of Laptops and Other Devices

- For which work-related tasks may I use my personal device (laptop, desktop, phone, tablet)?

  Work performed online without anything being downloaded may generally be

performed on personal devices; this includes accessing and responding to emails through a web browser, working in Canvas, attending virtual meetings, conducting research and accessing online resources, and reviewing non-sensitive academic materials. Personal devices may also be used to run software applications that do not contain sensitive Berry data.

- For which work-related tasks may I **NOT** use my personal device (laptop, desktop, phone, tablet)?

  Storing sensitive or sharing confidential information, including student records and financial data. Performing administrative tasks that require access to internal systems. However, a personal device may be used for these purposes by using Berry's VPN and remotely connecting into a Berry device to perform these tasks.

- May I use USB drives / thumb drives to store or transfer work-related files?

  USB drives/thumb drives are permitted for storing or transferring non-sensitive files. They are prohibited for storing or transferring sensitive or confidential information.

- If I do not have a portable Berry device (laptop, tablet, etc.) and need to work remotely without internet, how may I do so?

  Employees may not perform work-related tasks remotely that would require saving sensitive information on personal devices. Employees requiring a portable Berry device should contact the supervisor to discuss options.

- May student workers store sensitive Berry data on their personal laptops or other devices?

  Student workers and employees are prohibited from storing sensitive Berry data on personal devices. All sensitive data should be stored on institution-provided devices or secure, institution-approved storage solutions.

Use of Software/Services

- How should I communicate sensitive information to students?

  When communicating sensitive information to students, please use secure communication platforms approved by the institution (e.g. email, Canvas inbox). Avoid sharing sensitive information through unsecured channels such as personal email, text message, or social media.

- Is it a violation of this policy if my personal phone automatically backs up Berry emails or other sensitive Berry data?

  It is a violation of the policy if personal devices automatically backup Berry emails or other sensitive data to non-approved services. Please ensure backup services are disabled for work-related accounts on personal devices, or use institution-approved backup solutions.

- Why do I need to use Microsoft OneDrive for work-related tasks instead of a personal file-storage service like Dropbox or Google Drive?

  Files stored in Microsoft OneDrive using approved Berry College accounts help the institution to maintain control of confidential/sensitive data and documents, minimizing risks while improving both privacy and security. It also provides a more secure means of sharing sensitive data or documents than sharing by email or by removable flash drive.