Data Protection Guidelines

Data Protection Guidelines

Sensitive computer data is defined as names, addresses, social security numbers, any identifying bio-demographic information, institutional financial data, family financial data commonly found in financial aid applications and supporting documents, employee payroll and personnel data, corporate, foundation and individual donor data, and data concerning any other individual or independent entity.

As described in the W&J College Confidentiality Statement and the Password Policy, employees are responsible for:

- protecting and securing data they extract from a College owned database and placed onto any device including a College or personally owned computer, mobile computing device, or portable storage device, whether being used on Campus or from a remote or off Campus location,
- protecting and securing College owned data removed, printed or downloaded from a College or personally owned computer, mobile computing device, or portable storage device, and
- ensuring that account passwords remain private and sufficiently complex in accordance with the W&J Password Policy.

Employees are also responsible for ensuring that computers they are using remotely, whether College owned or personally owned, are updated with the most recent antivirus software, operating system releases, security patches, and application software updates.

Sensitive computer data, as defined above, should always be stored on the College's protected file server space. Employees with an ongoing demonstrated need should establish a secure connection, such as a virtual private network (VPN) connection or a secure remote desktop connection when remotely accessing sensitive data on College servers. Sensitive data should never be transmitted via email or in any other plain text or common format. IT Services can assist with secure, encrypted transmission of sensitive data.

College owned computers that are on campus and connected to the local area network are automatically updated with the most recent antivirus software, operating system releases and security patches, and application software releases. Employees who use College owned computers from remote locations should secure these updates on at least a weekly basis. Questions regarding these guidelines should be addressed to the ITS Helpdesk.