Confidential Data

Purpose

To protect confidential information vital to the University's business. Information includes but is not limited to: all transactional records, student and employee information, memos, reports, etc.

Policy Statement

All employees must safeguard University confidential business information as part of their daily actions and work routines. Confidential data is defined in the “Data Classification Standard” listed at the bottom of this policy.

Applies to

All employees

Responsibilities

- For authorized personnel confidential data may be made available on a need to know basis as and when required. For all other persons access to such information must be prohibited,
- Unauthorized modification, transmitting or other dissemination of confidential information is strictly prohibited. Unauthorized dissemination of this information may result in disciplinary or legal action as appropriate,
- Confidential information should be safely stored and protected while on file servers, network drives, workstations, and during any type of transmission. Authorized access should be enforced. Confidential information should be erased securely from network drives, file shares etc. after proper authorization.
- Network or directory share information showing where the confidential information is stored must not be publicly viewable,
- Confidential data must not be emailed or faxed; unless there is no other method available to transmit the information. Upon prior authorization, confidential information sent via email must be sent from their official Bridgewater State University (username@bridgew.edu) email account,
- Employees must not download and store confidential information unless encrypted on their personal computers, external hard drives, thumb/ pen drives and CD/DVD, or any removable device,
- Printed reports that contain confidential data must not be left available to the public. All printed confidential data must be shredded or disposed of into locked bins,
- Employees must not take printed or unencrypted confidential data off-campus,
- Employees must not discuss confidential data in public,
- All attachments or electronic files received from external sources must be scanned for viruses or malicious code in order to protect existing confidential information,

- The University will periodically audit employees to insure compliance and enforcement of policy,
- Any incidents of non-compliance may be reported to the Chief Information Officer (CIO).

Data Classification Data Classification Standards (PDF)

Title:	Confidential Data
Approved By:	President's Cabinet
Approval Date:	April 11, 2011
Date of Last Revision:	July 30, 2013
Policy Category:	Information Technology Division