

# PROCEDURE 2.16.0: DATA ACCESS – PRIVACY & SECURITY

## Confidentiality

Employees who have access to confidential information about Sandburg, its employees, students or donors may not communicate this information internally or externally to someone who doesn't have access to this information without prior written consent from the president or the cabinet. Such correspondence (e-mail or otherwise) should be marked "Confidential."

Unauthorized communication of employee or student personal information, such as the home addresses, phone numbers, Social Security numbers or protected information (e.g., FERPA, HIPAA, other state and federal laws) including, but not limited to accessing, transmitting, receiving, or seeking unauthorized, confidential or protected information is strictly prohibited.

## Temporary removal of confidential information from campus

There may be occasions when you may find it necessary to remove document(s), laptops, and removable storage devices containing confidential information and non-public private personal information from college premises. If sensitive data is transported in technology-readable storage media and devices, you must take reasonable precautions to ensure the security of the media and the information it contain including:

- Retaining direct secure control of the document(s), laptop and/or removable storage device.
- Not leaving confidential information (in any format) in vehicles.
- Encrypting electronic information coordinated and approved through Technology Services prior to transport off campus.
- When staying in a hotel, don't leave laptops, mobile devices, removable data storage devices and/or paper documents unsecured.
- Obtaining permission for removal of confidential information from your supervisor or Cabinet.

## Report of missing/stolen data

Missing and/or stolen data must be reported immediately to your supervisor and Technology Services. Timeliness of reporting missing and/or stolen data is vital to ensure the protection of both the college and individual employee's personal data.

*Original: 8/06*

*Reviewed: 5/16, 12/17, 1/24*

*Revised: 5/16 12/17, 1/24*