Procedures for the Secure Handling of Social Security Numbers and Other Sensitive Information

SCOPE

The procedures noted herein apply to all members of the New Jersey City University community, including but not limited to all employees, both permanent and temporary, contractors, vendors, and any others entrusted with social security numbers (SSN) and other sensitive information.

PURPOSE

All members of the University community are responsible for protecting and securing University data and personal information pertaining to students, faculty, and staff. It is essential that anyone who handles social security numbers and other sensitive information adhere to procedures for the secure handling of such information. Examples of sensitive information include, but are not limited to, social security numbers, credit card numbers, bank account information, and date of birth. The following procedures should be followed when handling and exchanging sensitive University information.

Secure Handling of Electronic Files Containing Sensitive Information

- All files containing social security numbers and other sensitive information must be encrypted with a password when not in use. Please see Data Encryption procedures below.
- Do not store files containing social security numbers or other sensitive information on personal computers, laptops or other devices, including smartphones or tablets. Instead, this information should be encrypted with a password and stored on University network drives secured with limited access to those required to use this information in the course of their job function.
- Do not store files containing social security numbers or other sensitive information on cloud-based file storage systems (e.g., Dropbox, Google Drive, etc.).
- Do not use email to send unencrypted data files or reports with sensitive information internally or externally.
- Never send data files containing sensitive information, unencrypted or otherwise, via Hotmail, Yahoo, Gmail or other similar email accounts.
- Never share your GothicNet ID and password with anyone.
- Never login to GothicNet and allow anyone else to access the system using your credentials.
- If files containing sensitive information must be transmitted to external locations such as federal and state agencies and banks, the following procedures should be followed:
    - Request an ID and password from the recipient to transmit the information via a secure file transfer protocol (SFTP) or secure website (HTTPS).

  - If you must email data files containing sensitive information to external recipients, email an encrypted file that is password protected. Have the recipient call you for the password to decrypt the file.
- Determine the retention period for the data file and delete the file after the retention period has ended. See *State of New Jersey Records Retention Schedule: S510000-001 thru S511014-001 Four Year Colleges* for specific information.

Data Encryption Procedures

- Use the WinZip software application to encrypt and password protect a single file or a collection of files containing sensitive information. WinZip can be obtained by placing a request through the IT Help Desk. See "How to Encrypt a file in WinZip" for instructions
- Excel files containing sensitive information can be secured using the provided encryption and locking feature. See "How to Encrypt an Excel Workbook" for instructions.
- To open a file encrypted in WinZip, see "Decrypt a WinZip Encrypted File".
- For a current copy of WinZip or additional help with file encryption, please contact the NJCU Help Desk.

Secure Handling of Paper Documents Containing Sensitive Information

- Limit the printing of documents containing sensitive information and ensure documents are placed in a safe location.
- File cabinets containing sensitive information must be kept locked when not in use.
- Filing of documents containing sensitive information should be assigned and restricted to authorized permanent employees.
- Printed documents containing sensitive information should be maintained only as long as necessary and should be shredded by authorized permanent employees using a cross-cut or micro-cut shredder. See "*State of New Jersey Records Retention Schedule: S510000-001 thru S511014-001 Four Year Colleges*.