UNIVERSITY OF NOTRE DAME

Information Handling Standard for Bank Account Numbers
Version 1.0

1. Introduction

This standard establishes the University practices for bank account numbers when handled, stored, sent, received, or accepted by the University of Notre Dame in combination with a security code, password, or access code that would allow access to a bank account.

2. Standard

1. All University use of bank account numbers combined with a security code, password, or access code (henceforth referred to as bank account numbers), on campus must be done as part of an approved business process. Use of bank account numbers for personal use is done at the individual's discretion.

2. Paper records
   - 2.1. Papers and forms containing bank account numbers must be kept in a physically secured location such as a locked cabinet and/or office in accordance with their records retention schedule.
   - 2.2. When bank account numbers are not required on an ongoing basis:
     - 2.2.1. The bank account numbers must be redacted with a black permanent marker or whiteout. The original document must then be photocopied, and the copy retained while the original is securely shredded.
     - 2.2.2. Paper records that are not required on an ongoing basis must be securely shredded by placing it in University provided secure shred bins, or by use of a crosscut shredder.

3. Electronic records
   - 3.1. Electronic records containing bank account numbers must be stored in CORPFS, or another filesystem or application approved by the Information Governance Committee for storage of highly sensitive data. Unencrypted local drives may not be used for storage of bank account numbers.
   - 3.2. Access of electronic records containing bank account numbers must be restricted to only those users with a business need to access the data, and such access must be periodically reviewed and updated to ensure that it is only stored if there is an IGC approved business reason or process that requires it.
   - 3.3. Electronic records containing bank account numbers must be securely erased when disposed of using a University approved secure erase tool.

4. Transmission
   - 4.1. Electronic transmission of bank account numbers must be done in an encrypted form, using encryption methods on the University's list of approved encryption methods.
   - 4.2. Email or file transfer must be done only with the file encrypted. Passwords must be transferred under separate cover.

5. Removable media
   5.1. Bank account numbers stored on removable media such as USB removable drives ("thumb drives"), CD, DVD must
      5.1.1.1. be stored in an encrypted form as individual files OR be stored on encrypted media and
      5.1.2.must use password protection

6. Retention schedule
   6.1. Bank account numbers collected and stored as part of an approved business process must have a designated retention schedule in compliance with the University records retention schedules found at http://archives.nd.edu/records
   6.2. Retention schedules must have a plan to destroy or archive the SSN data with the University archives.

3. Definitions

Approved business process	An approved business process must be approved by the Information Governance Committee and must have a business process document on file, and appropriate security and access controls in place for the process.
Bank Account Number	The account number for a bank account or similar financial account.
Security code, Password, or Access code	The code or password that allows access to a bank account, which, in combination with a bank account is designated as highly sensitive information.
Secure Erase	Electronically shredded using a program such as Eraser, DBAN, Identity Finder's shred capability or the MacOS secure file delete facility.
Secure shred	Shredded using a crosscut shredder, or by placing the document in one of the campus provided secure shred bins.
University network	Networks that Notre Dame owns and maintains