UNIVERSITY OF NOTRE DAME

Information Handling Standard for Driver’s License Numbers
Version 1.3.2

1. Introduction

This standard establishes the University practices for Driver’s License numbers handled, stored, sent, received, or accepted by the University of Notre Dame.

2. Standard

1. All University use of driver’s license numbers (henceforth “DLN”) on campus must be done as part of an approved business process. Personal use of driver’s license numbers is done at the individual’s discretion.

2. Paper records
    - 2.1. Papers and forms containing DLNs 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 DLNs are not required on an ongoing basis:
        - 2.2.1. The DLNs 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.
            - 2.2.2.1. In cases where a driver’s license number is required for special travel requirements, copies must be used only for that requirement, and should be disposed of after 1 year, or after the travel requirement is met, whichever is shorter.

3. Electronic records
    - 3.1. Use or storage of electronic copies of driver’s license numbers or records containing driver’s license numbers must be approved by the Information Governance Committee.
    - 3.2. Electronic records containing DLNs 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 DLN.
    - 3.3. Access of electronic records containing DLNs 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.
    - 3.4. Electronic records containing DLNs must be securely erased when disposed of using a University approved secure erase tool.

4. Transmission
    - 4.1. Electronic transmission of DLN 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. DLN stored on removable media such as USB removable drives (“thumb drives”), CDs, or DVDs must be
      5.1.1. 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. Driver’s license 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 DLN 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.
Driver’s License Number	Driver’s license numbers are unique identifiers issued by states as part of the process of licensing a driver. The format and length of these numbers varies from state to state.
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