

RETENTION TIPS

A file naming convention can incorporate retention requirements as an extension of the Availability data classification.

First specify a retention period:

- Relative: **Y4**, meaning retain the file for 4 years after data was active
- Absolute: **20120630**, meaning retain the file until June 30, 2012.

Next specify a disposition for expired data:

- **A** – archive file
- **D** – securely destroy data
- **H** – hold for historical review
- **P** – retain file permanently

Such a naming convention makes it easier for a system administrator to periodically search folders and “harvest” files for archival or secure deletion.

Examples

Sample file names using both classification *and* retention schemes:

year-end report CIA(HHL_Y4D).doc,
retain document for 4 years since active and then securely delete it.

Campus pics CIA(LLL_20120630H).jpg,
retain file until June 30, 2012 and then review for it for historical value.

More ... www.bgsu.edu/infosec



MANAGING **SENSITIVE** DATA

PRIVACY

POLICY

BGSU employees are required to protect the confidentiality and privacy of data.

The BGSU Code of Ethics and Conduct also reminds us that “we must act in a way to inspire public confidence in the honesty and integrity of our actions.”

ITS Network
& Computer
Policies #A27

[www.bgsu.edu
/downloads/cio
/files9602.pdf](http://www.bgsu.edu/downloads/cio/files9602.pdf)

SENSITIVE DATA

Sensitive University data should be *identified, located, and labeled*.

What is sensitive? Sensitive information includes, but is not limited to:

- Social Security Numbers,
- driver license numbers,
- credit card or other financial account numbers,
- BGSU ID numbers,
- health data,
- financial data,
- education records,
- intellectual property or research, or
- any information that could harm individuals or the University if publicly exposed.

The Ohio Breach Notification Act requires prompt notification to residents whose personal data has been exposed.

www.legislature.state.oh.us/bills.cfm?ID=126_HB_104

DATA CLASSIFICATION TIPS

Classify sensitive data according to the following data management requirements:

- **C**onfidentiality – ensuring only authorized access & disclosure
- **I**ntegrity – ensuring authorized modification or destruction, non-repudiation, and authenticity
- **A**vailability – ensuring timely and reliable access

FIPS PUB 199

Standards for Security Categorization of Federal Information and Information Systems

<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

For details, see the following publication:

Next, assign impact levels to each of the preceding CIA classifications that assess the impact of breaches or exposures to the organization or affected individuals:

- **L**ow
- **M**oderate

- **H**igh

Now by labeling files when they are created, you will readily know which data requires special care in handling. One simple technique is to include the data classification (all caps) in the file name:

Summary Report CIA(HHL).xls

The label informs you that the spreadsheet has **H**igh **C**onfidentiality, **H**igh **I**ntegrity, and **L**ow **A**vailability requirements.

Never copy such a file to a flash drive or laptop, and transport it from a secure office location without encryption!

With high integrity requirements, you would only allow the original file to be modified, set the attributes of copies to read-only, know who has copies and notify them when changes occur. Copies then always match the original.

Low availability could mean that the data is usually not required immediately.

RECORDS MANAGEMENT

Ohio law requires that University data be retained according to a records retention schedule.

For more information, refer to the following

Records Retention Information

<http://www.bgsu.edu/colleges/library/cac/uarchives/ecman.html>

BGSU web site:

