



Cybersecurity Assistance for Nonprofits

Data Classification Toolkit:

A Quick Start Guide for Nonprofits

January 2026 Edition



501Secure is a nonprofit program of The Piper Center for Nonprofit and Civic Impact at the Mable G. Ragland Institute in Spokane, Washington.

Questions about this guide or 501Secure program services contact:
info@501Secure.org

All rights reserved. **Mabel G. Ragland Institute** 2026

Table of Contents

Toolkit Contents	4
Introduction	5
Benefits of an Asset Inventory	6
The Current U.S. Data Security and Privacy Law Mosaic	6
<i>Resources for Staying Current</i>	7
<i>Data Privacy Laws</i>	7
<i>Data Security & Breach Notification Laws</i>	7
Completing a Collaborative Data Inventory	8
<i>Classification Taxonomy</i>	9
Table 1: Data Classification Taxonomy	9
<i>Data Handling Guidelines</i>	10
Table 2: Example Data Use Guideline Matrix	10
Privacy vs. Confidentiality	10
What is Confidentiality, Integrity, and Availability?	11
Defining “Sensitive” Information for Your Organization	12
<i>The Number and Type of Records Matters</i>	13
Data Breach Assessment Tool	14

Toolkit Contents

You'll find the following files included in the *Data Classification Toolkit (501Secure).zip* file:

Data Classification Toolkit: A Quick Start Guide for Nonprofits

Asset Inventory Template Excel Workbook

Data Handling Guidelines PowerPoint Template

Introduction

A nonprofit gains the most value from identifying and classifying its data when the process is led by a cross-functional team. Every department from admin to programs to development offers unique insights to help protect the organization's collective impact. A collaborative effort across your entire organization brings a wide range of rewards. When program staff, fundraisers, and administrators work together, you get an accurate view of your data—uncovering "shadow data" hidden within personal spreadsheets or forgotten paper files that a solo audit would miss. This collective effort tends to reveal surprising information about where data is **actually** stored and how it is used and by whom.

Classifying your data will help you decide which information needs a simple password and which requires encryption and special data handling.

For a small team, a data classification project can quickly become overwhelming, so it is best approached as a step-by-step process. This guide will walk you through:

- Parsing the difference between privacy and confidentiality
- Identifying and situating your organization's compliance responsibilities amidst the complex mosaic of state and federal data privacy laws
- Organizing a collaborative asset inventory project with your team
- Setting a guiding definition for sensitive data
- Creating a matrix for data classification and data handling
- Developing a tool to quickly triage data incidents to determine if data breach notification may be required.

This guide is not intended as legal advice. It is a primer to help you get started. As you move through these sections, remember that you don't have to have all the answers at once. Data discovery and classification initiates conversations, heightens security awareness, and prompts changes in workflows and data handling over time. Expect to spend several weeks or months on the initial phases of this project. We are here to answer your questions, help@501Secure.org.

Benefits of an Asset Inventory

The time and effort invested in inventorying your organization's assets and classifying your data will provide many functional benefits. It can be used to plan and guide the security of your hardware, cloud accounts, processes, and data. It will support planning around meeting state, federal, regulatory, and contractual privacy and data security responsibilities.

Beyond data security and compliance, it can guide security awareness training, business continuity planning, and risk management decisions. An inventory can reveal information flow issues, redundancies, vulnerable business processes and services, and initiate conversations that can lead to improved organizational efficiency and transparency.

The Current U.S. Data Security and Privacy Law Mosaic

Consumer data security and privacy in the United States is regulated by a complex system of state and federal laws, some governing data privacy and other laws that set standards for data security and breach notification.

It is important to identify the distinctions between data privacy and data security and breach notification laws, as they require different types of planning and compliance. A list of applicable laws and regulations relevant to your organization should be updated at least annually to ensure your team remains aware and compliant, as these laws are constantly being shaped in real-time by court cases that test the limits of their interpretation and applicability.

Resources for Staying Current

Because the legal landscape shifts so quickly, we recommend using these two trusted resources to help you update your compliance list annually:

- [IAPP \(International Association of Privacy Professionals\)](#): This is a global nonprofit dedicated to data privacy. They offer a specific nonprofit membership (roughly \$110/year) which provides access to updated charts of state laws, professional research, and a community of privacy experts.
- [NCSL \(National Conference of State Legislatures\)](#): Their website offers a free, reliable database of current and pending state legislation. It is an excellent place to see which states are currently debating new privacy or breach notification bills.

Data Privacy Laws

Data privacy laws generally seek to regulate consumer data collection and stewardship to promote transparency and consumer control. They give individuals rights over their personal information—such as the right to see the data collected, the right to correct it, or the right to ask that it be deleted.

Data Security & Breach Notification Laws

All [50 states](#) have data security and breach notification laws. They mandate that you take reasonable steps to secure data and specify how and when you must notify people if that data is stolen or leaked. One state might require you to notify people within 30 days, while another might require 45 days. Some states include medical information or biometrics in their definition of "sensitive data," while others do not.

Like the GDPR, some of these laws apply based on where the *person* lives, not where your nonprofit is located or their data is stored. For example, if you have donors or clients in New York, data about them may be subject to that state's specific privacy rules, regardless of where your database is located.

Completing a Collaborative Data Inventory

Before you can protect organization data, you must know what you have. An inventory is the first step. Use the Asset Inventory Template included in this toolkit to help your team complete steps 1 through 3:

1. Inventory organization information and private data; its location; who has access to it; what its used for
2. Classify data (public, internal, confidential, restricted) to prioritize and select your security efforts
3. Assess Risk by estimating impact of the loss of confidentiality, availability, or integrity of that data

Once you've completed your inventory, you'll be ready to put the information you've gathered into action:

4. Clean Up by determining planning to address data that is no longer needed, relocating or securing sensitive data, creating guidelines and training staff in safe data handling procedures to reduce the risk of a potential breach.

Classification Taxonomy

A data classification framework helps nonprofit teams protect their data by grouping information into 3–5 levels based on sensitivity. Each level is identified with a category name, a description of the data, and real-world examples relevant to the organization (such as donor records or grant proposals). Data classification levels and the results of an asset inventory can be combined to create data handling guidelines, which can be written and distributed as both a formalized organization-wide policy and a data handling quick reference guide.

Also see [NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#) and [Microsoft's Data classification and sensitivity label taxonomy](#)

Table 1: Data Classification Taxonomy

Level	Classification	Description	Typical Examples
L1	Public	Information intended for the public.	Newsletters, public website content, brochures.
L2	Internal	Routine operational data; not for public eyes, but low risk.	Internal memos, staff directories, meeting minutes.
L3	Confidential	Sensitive information that could harm individuals or our reputation.	Donor lists, home addresses, non-public grant drafts.
L4	Restricted	Highly sensitive data with legal or safety implications.	SSNs, credit card info, health records, case files.
L5	Sensitive	Defined by your organization.	<i>Information that would result in substantial harm, embarrassment, inconvenience, or unfairness to an individual or organization.</i>

Data Handling Guidelines

Table 2: Example Data Use Guideline Matrix

Data Level	Storage	Internal Sharing	External Sharing	Access Control	Disposal (Digital & Physical)
Level 1 (Public)	Any org-approved cloud drive (Google Drive, SharePoint).	Can be emailed or shared via internal links.	Standard email or shared links.	Open Access: All staff, volunteers, and the public.	Standard digital deletion and office recycling.
Level 2 (Internal)	Any org-approved cloud drive (Google Drive, SharePoint).	Can be emailed or shared via internal links.	Standard email or shared links.	All staff.	Standard digital deletion and office recycling.
Level 3 & 4 (Confidential/Restricted)	Secure folders only. Never on personal USBs or unencrypted laptops.	Only with staff who have a legally required "need to know."	Password-protected or secure links. Never in email body.	Role-Based: Specific depts (HR/Finance) or Project Leads only.	Permanent digital delete (empty trash); Crosscut shred physical docs.
Level 5 (Sensitive)	Secure folders only. Treat as high-risk if disclosure causes harm or embarrassment.	Limited to relevant project teams or managers.	Must use secure, tracked links. Use passwords if sent externally.	Need-to-Know: Access restricted to those actively working on the file.	Permanent digital delete (empty trash); Crosscut shred physical docs.

Privacy vs. Confidentiality

While often used interchangeably, these are two distinct concepts:

- **Privacy is about the person.** It is the right of an individual to have control over how their personal information is collected, used, and shared. When you respect privacy, you are respecting the person's autonomy.
- **Confidentiality is about the data.** It is the duty of your organization to protect information from being seen by unauthorized people. If privacy is the "right" to be left alone, confidentiality is the "lock" you put on the file cabinet.

What is Confidentiality, Integrity, and Availability?

Confidentiality is about ensuring that sensitive information is accessible only to authorized individuals. For a nonprofit, this means protecting donor details, client records, and internal strategies from unauthorized disclosure. By classifying data based on its sensitivity, you can apply the right level of access controls to prevent private information from falling into the wrong hands.

Integrity focuses on maintaining the accuracy, consistency, and trustworthiness of your data over its entire life cycle. It ensures that information has not been altered or deleted by unauthorized users or accidental errors. Proper data security measures guarantee that when you pull a report on program outcomes or financial records, the information is correct and can be relied upon for decision-making.

Availability ensures that information and systems are ready for use when the organization needs them. Whether it is a database of volunteers or a grant application portal, data is only valuable if it is accessible to your team. Availability may be impacted by service disruptions caused by hardware failures, cyberattacks, technical glitches, or natural disasters. Keeping data backups and creating back up processes when data or services are unavailable help keep your organization running during unexpected disruptions. An asset inventory helps to identify the data, software, and processes most critical to your organization's functioning.

Defining “Sensitive” Information for Your Organization

The classification “sensitive” is often used interchangeably with restricted (i.e., personally identifying information protected by law) requiring the highest protection level. However, sensitive information does not always fall under government or industry regulatory oversight. Sensitive information can be contextual. For example, first and last name and email address generally do not fit the definition of sensitive information for most state laws, but in the context of your organization, if this information for two dozen persons appeared in a file labeled “employees currently being investigated for sexual harassment”, the information becomes sensitive.

The Department of Homeland Security suggests using the following question to help identify sensitive information:

Would the unauthorized disclosure of personal identifiable information result in substantial harm, embarrassment, inconvenience, or unfairness to an individual (organization)? If yes, or if you are unsure, assume it is Sensitive PII.

Your organization must adopt a clear, guiding definitions for restricted, confidential, internal, and sensitive information. These definitions serve as the foundation for how data is handled and, more importantly, provides an initial, internal yardstick for determining whether a reportable "breach" has occurred. Your primary source for defining restricted data should be the laws of the state where your organization is headquartered. However, because data is often "borderless," you must also look at where your data subjects live and the kinds of data you collect and store, and how it is routinely used and shared outside your organization.

As you inventory your databases, you must determine if you hold records belonging to residents of other states. If you do, those states' privacy laws (which define what information is sensitive) and breach notification laws (which define when you must sound notify affected individuals and state agencies) may apply to those specific records.

The Number and Type of Records Matters

The scale of your data and the kind of data you keep must play a role in whether you need to incorporate applicable state definitions of sensitive data into your own organization-wide policy.

Example: [New York's SHIELD Act](#)

Imagine you are a nonprofit in Ohio. Your donor database contains 12 records belonging to residents of New York.

- **Sensitive Data Definition:** New York's SHIELD Act has a specific definition of "private information" that includes "any personal information concerning a natural person in combination with any one or more of the following data elements in combination any required security code" (i.e., Social Security number, driver's license number, account number, biometric information, username or email address, and password credentials).
- **Notification Threshold:** If an unauthorized person accesses those 12 records, the SHIELD Act requires you to notify the New York Attorney General (AG) only if the breach affects over 500 residents **and** the records meet the law's definition of private information.
- **Impact:** Because you only have 12 records, you wouldn't be required to report the incident to the State of New York because the records did not contain data defined as private information and the number of records did not meet the breach notification threshold. However, you would likely not be required to notify those 12 individuals directly if their data was accessed because the records do not contain data that meets New York's private information definition.
- **Strategy:** In this case, you wouldn't necessarily need to overhaul your entire organization's definition of restricted or sensitive data just to match New York's law for 12 people. However, you must be legally aware that the law exists and take reasonable precautions to protect those records. If that number grows to 500, it may be time to incorporate that state's definitions into your breach notification triage tool (next page).

Data Breach Assessment Tool

Here's an example from Washington state for use by state agencies. You can see the format of basic questions to complete an early triage to determine whether an incident is a breach that requires notification. Because breach notification laws have a specific period by which notification must occur, it is imperative to assess whether an incident is reportable as quickly as possible.

[RCW 42.56.590 Breach Assessment form](#)

Assembling a guiding document based on your state's laws can be a good place to start when initially reviewing the severity of an event. Disclosures are not always breaches by cyber criminals. A staff member may accidentally share confidential or restricted information with a vendor, case worker, or agency. Some state data notification laws make a distinction between a complete loss of control of data versus an inadvertent disclosure to a trusted entity during the normal course of business that is unlikely to create harm.