SMALL BUSINESS DATA CLASSIFICATION HANDLING POLICY

A practical guide for protecting your business technology assets.

Document Owner: [Your Name]
Effective Date: [Current Date]
Version 1.0

Contact Info:
Michael Nichols
manichols936@gmail.com
Connect/message me on LinkedIn

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.

[Company Name] Data Classification Handling Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0							

Disclaimer: This sample policy has been provided by Michael Nichols as a generic document to support the enhancement of your security posture. It is based on security frameworks, SOC 2 and NIST CSF, and has been adapted specifically for small business use. It is unlikely to be complete for your organization without customization. This document is not legal advice and I am independent of a registered CPA firm.

1. Purpose

This policy establishes a simple framework for classifying <Company Name>'s data based on sensitivity, value, and importance to our business. By properly classifying our data, we can implement appropriate security measures to protect it while balancing security needs with practical business operations.

2. Scope

This policy applies to all employees, contractors, and partners who have access to <Company Name>'s data. Everyone who handles company information is responsible for following these guidelines to protect our data appropriately.

3. Data Classification

Data classification categorizes information based on sensitivity and potential impact to <Company Name> if compromised. This helps determine appropriate security controls. All data should be classified as:

Restricted Data

Information whose unauthorized disclosure could cause significant risk to the company. Examples include data protected by regulations or confidentiality agreements. Apply the highest level of security controls to Restricted data.

Private Data

Information whose unauthorized disclosure could cause moderate risk. By default, all company data not explicitly classified as Restricted or Public should be treated as Private. Apply reasonable security controls.

Public Data

Information whose unauthorized disclosure would cause little or no risk, such as press releases and pricing. While minimal controls are needed for confidentiality, some protection against unauthorized modification is required.

Classification of data should be performed by appropriate Data Stewards - senior-level employees of <Company Name> who oversee the lifecycle of one or more sets of <Company Name> data.

4. Data Collections

When classifying data collections, use the most restrictive classification of any individual element. For example, if a collection includes both public information (name) and restricted data (SSN), classify the entire collection as Restricted.

5. Reclassification

Periodically review data classifications to ensure they remain appropriate as legal obligations, usage, and value change. Annual evaluation is recommended, but Data Stewards should determine appropriate frequency. If classification changes, analyze security controls for gaps and address them promptly based on risk level.

6. Calculating Classification

The goal of information security is protecting the confidentiality, integrity and availability of <Company Name> data. Data classification reflects the impact level if any of these are compromised.

There's no perfect formula for classifying data. Some classifications are obvious, such as when federal laws mandate protection of certain information (e.g., personally identifiable information). If classification isn't clear, use the following table as a guide. Note that it is an excerpt from the Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology (NIST), which discusses the categorization of information and information systems.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

As the total potential impact to the <Company Name> increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Information Security Office for assistance.

7. Related Standards, Policies, and Processes

- Information Security Policy
- Acceptable Use Policy
- Vendor Management Policy
- Incident Response Policy

8. Definitions and Terms

The following definition are not all-inclusive and should be updated as new information is made available:

Term	Definition
Confidential Data	A generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with sensitive data.
Data Steward	A senior-level employee of <Company Name> who oversees the lifecycle of one or more sets of company Data. See the Information Security Roles and Responsibilities for more information.
<Company Data>	All data owned by <Company Name>
Non-Public Information	Defined as any information that is classified as Private or Restricted Information according to the data classification scheme defined in this Guideline.

Sensitive Data	A generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with confidential data.

Appendix A – Predefined Types of Restricted Information

The following are defined types of Restricted data based on state and federal regulatory requirements:

Authentication Verifiers

An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to:

- Passwords
- Shared secrets
- Cryptographic private keys

Covered Financial Information

See the Federal Trade Commission's website to understand how to comply with Gramm-Leach Bliley Act and what constitutes covered financial information here.

Electronic Protected Health Information ("EPHI")

EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For the purpose of this definition, electronic media includes:

- Electronic storage media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

- Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks and the physical movement of removable and/or transportable electronic storage

media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exists in electronic form before the transmission.

Export Controlled Materials

Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State.

Federal Tax Information ("FTI")

FTI is defined as any return, return information or taxpayer return information that is entrusted to the <Company> by the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.

Payment Card Information

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

Personally Identifiable Information ("PII")

For the purpose of meeting state security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- State-issued identification card number

- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

Protected Health Information ("PHI")

PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component. PHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age (if over 89)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual