RECORDPOINT

Content Brief

Project	SEO post – Data classification
Author	
Date	26/5/22
Agency	Terry O Faulkner
Deadline	+ 1 week from confirmation

Purpose:

Create a blog post to increase our rank for the keyword: “confidential vs sensitive information”

Production Specifications:

Suggested title	A guide to data classification: confidential vs sensitive vs public information
Keywords to include	Social security unauthorized access unauthorized disclosure potential harms identity theft protection law Confidential Information control of access level of sensitivity sensitivity level privacy laws email address

Headings	security confidentiality sensitivity privacy classification permission message agreement Confidential Information sensitivity level
Suggested structure	Intro Why classify your data? (classification) What is sensitive data? Examples of sensitive data Categories of sensitive data What is confidential information? Categories of confidential information Data privacy laws
CTA	See how RecordPoint solves your data categorization challenges. Schedule a demo https://www.recordpoint.com/demo-request/
Length	1.1k words

What are the mandatories?

- Please use US English. Sentence case for headings. This is how you the correct spelling for: RecordPoint
- The message should complement the messages currently in field.

A guide to data classification: confidential vs. sensitive vs. public information

Data classification is the process of grouping information according to needs. By classifying data, we can search more effectively, manage high-value content and protect it from unauthorized disclosure. In this post, learn why it's important to classify your data, know four standard classifications for data, and how automation can reduce the number of steps you can take in keeping your company's data safe and eliminate potential harms.

Why classify your data?

Classifying your data is essential for several reasons. First, it helps you determine what kind of information you are storing, the value that information has to your organization, its criticality to your business process, and how it can be used if lost or hacked. In addition, knowing what type of data you are dealing with will help you make more informed decisions about where to store the information on your computer system and the nature of controls that are required based on classification. Finally, it also makes life easier when dealing with compliance regimes such as financial regulations and audit requirements. Information like credit card numbers and personal information (especially sensitive information) must be handled differently and with additional controls applied.

Data Classifications

There are four commonly used types of data: public, internal, confidential, and restricted. Different industries have more granular standards and definitions. For example, in government and highly regulated industries (financial, banks, healthcare) there are often 5 levels: Top Secret, Secret, Confidential, Sensitive, and Unclassified.

Almost any type of data can be classified as sensitive. Credit card numbers, bank account numbers, and driver's license numbers are all examples of sensitive data. So are birth dates and email addresses. IT teams will generally classify data in these ways:

- *Public* data poses little-to-no risk if disclosed, as anyone can easily access it. For example, school directories, the White pages, or your business's consumer prices would be classified as public information. This data is not considered sensitive.

- *Internal* data isn't intended for publication, though it may be accessed under Freedom of Information (FOIA) or similar legislative regimes. This should be assessed to gauge potential harm, though this is likely to be minimal. Examples include your business' organizational flow chart or IT provider data.

- *Confidential* data must remain private and protected accordingly. Leaking of this kind of data (which could include social security numbers, medical records, bank account numbers or employment contracts) could cause serious financial, legal, or regulatory consequences.

- The most sensitive data is *restricted*. Exposure of this data could have serious financial, legal, or regulatory consequences for your business. This classification requires additional controls and is likely subject to additional security standards. Protecting data like law enforcement records and data relating to mergers and acquisitions should be taken seriously.

What is sensitive data?

Sensitive data is usually any private information you must protect from loss or information that, if released, could cause damage to your organization’s reputation or operations. This includes physical and digital formats like documents, photographs, videos, or audio. Most businesses have sensitive data collected in their network and are required to follow federal compliance laws.

For this purpose, we can broadly define sensitive information as anything that can cause harm, embarrassment, inconvenience, or unfairness to an individual or business if it is exposed or gets into the wrong hands.

Examples of sensitive data

Sensitive information comes in many forms, but the most common is personally identifiable information (PII), and personal or nonpublic personal information. PII can also be used to identify an individual and is protected under both state and federal law. In many jurisdictions, it is also carefully monitored, and non-compliance punished Examples include names, addresses, Social Security numbers, driver's licenses, and credit cards. Medical information, bank account numbers, or passport numbers are also considered sensitive data.

PHI is considered sensitive data because it can be used to identify individuals and their medical conditions. The unauthorized release of PHI can harm the individuals involved, causing them to lose their insurance coverage or suffer discrimination in employment or other areas. Therefore, organizations that handle PHI are required to take steps to protect the information from unauthorized access or use.

It is crucial to protect sensitive data from unauthorized access or use. Organizations subject to compliance regimes will need to ensure a security plan and the appropriate controls in place to ensure compliance and protect the information your customers or employees have entrusted you with. You can do this by implementing security measures such as firewalls, password protection, encryption, regular penetration testing, ensuring your cloud applications have the appropriate certifications (eg SOC2), and importantly training your employees to handle sensitive data securely. You should back up your data regularly to ensure its safety in case of a hack or other cyberthreat.

What is confidential information?

Confidential information is data that is not accessible to everyone. It's often private, but not always. Confidential information can be anything from your credit card number to patent applications.

Your business definition could be any information, knowledge, or data related to the operation of your business that is not in the public domain or otherwise publicly available. You designate confidentiality. Here are some examples:

- Proprietary Information
- Financial Information
- Medical Information
- Trade Secrets
- Personal Information

Data privacy laws

Data privacy laws are the rules and regulations that determine how a company may use, store, and share personal information. These laws are designed to protect against identity theft, fraud, and other crimes, ensure confidentiality among and between teams, and keep privacy worries at bay. They also control how businesses interact with customers in general by dictating methods of collecting information about and how businesses can use collected data.

For example: if a customer is shopping online with a vendor, they might click "I agree" to the terms of service before completing a purchase. Those terms of service include how long they keep track of order history and where they store data (on servers all over the world). Shoppers also agree not to use vendor services illegally (like reselling products purchased on their site). Finally, their terms often outline an arbitration clause stating that if disputes arise between users or between users or the vendor themselves, both sides will have to settle outside the courts or without legal action.

This information is governed by data protection legislation, which sets out the rules for handling information about individuals. It’s important to remember never to reveal personal details or share confidential business information unless necessary. The best practice would be to consult with your company's legal team before sharing any related to company activity in public channels such as social media platforms or newsletters.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to the United States, defines Personal Health Information (PHI) as individually identifiable health information. Protected health information includes demographic information about the individual, such as name, age, and sex; information about the individual's health history, including mental health conditions; and the results of any tests or examinations performed on the individual.

The General Data Protection Regulation (GDPR)

The GDPR is a European Union data protection law that gives EU citizens more control over their personal data. It applies to any company that targets or processes the personal data of individuals in the EU, regardless of where the company is located. Companies that process the personal data of EU citizens must comply with the GDPR which means if you have employees who are EU nationals, or you provide or leverage a product or service that can be accessed by EU citizens this applies to your business.

Businesses subject to the GDPR must secure explicit consent from individuals before collecting, using, or sharing their personal data. They must also provide individuals with clear and concise information about their rights under the GDPR, and ensure that individuals can easily exercise their rights.

Auto classification means more actionable insights

Auto classification is quickly becoming a must-have technology as organizations of all sizes are collecting more data than ever before. This influx could make it difficult for your business to understand the data to make the right choices. Fortunately, RecordPoint can help.

The RecordPoint Intelligence Engine offers automated records management that enables you to mark personally identifiable information (PII) and payment card industry (PCI) information consistently and at scale, with greater speed and accuracy.

CTA:
[Get Started on your journey to data classification today]