The 11 most common mistakes that derail data classification projects

Janusnet

In the digital era, users generate more information globally than ever before. Among those petabytes, every organization holds some data types that need safeguarding, whether personnel information, a customer database, a price list, intellectual property, or something else.

Strategically minded organizations increasingly use data classification (also known as protective markings, sensitivity labels, and security classification marking) solutions to improve how their teams and systems identify, track, store, retrieve, share, and control sensitive information. Cost-effective and straightforward to deploy, use, and maintain, data classification solutions are proven to reduce the risk of information loss or mismanagement and meet compliance requirements.

Our team has over 15 years of experience working with data classification solutions globally. This article shares 11 of the most common mistakes we see that derail data classification programs.

1. Too many/few classifications

Data classifications must reflect the sensitivity of an information file type and the likely consequences for your organization, should it fall into the wrong hands. The markings must make sense to all employees, including new hires and temporary staff, to help ensure accurate, consistent usage.

Define too many classification categories and users will get overwhelmed with choice, need help with application, or make mistakes. Defining too few makes life easier for users but risks your system under-protecting or over-protecting information.

To keep data classification processes specific, simple, and effective, we encourage every organization to understand its use cases and design practical classification schemas that fit those needs. For commercial organizations, start with a standard framework of three to four classification levels and tailor from there as needed.

2. Efficient data classification solution

As with all technology, not every data classification solution is created equal. Avoid over-complicating your data classification program by focusing on your organization's use cases and minimizing distractions from fancy "bells and whistles" that may offer eye-catching but unneeded capabilities. If a vendor offers to throw in data classification for free on top of other technology subscriptions, take a closer look to ensure it's the right fit for your needs. Most ‘free’ data classification packages deliver basic functionality bound into a wider security platform. Above all, aim for great integration with existing and planned security infrastructure. Complex selection, unlikely use case scenarios, and extra reporting waste precious budgets and team time and may not deliver the outcomes your organization needs.

See how fast and easy it is to classify data with Janusnet in our short video.

3. No good reason for classification

Effective and efficient business operations rely on information sharing. When considering a data classification program, stay mindful that only sensitive information needs dissemination controls. Applying complex labels to every bit and byte of information unnecessarily slows business processes. Avoid the mistake of applying data classifications for no good reason by clearly defining why you need classifications, including any compliance statutes or regulations, and how your existing IT infrastructure will handle them.

4. Users don't understand the benefits

Some technologists get over-excited by all the possibilities of a new solution. No wonder! Your new data classification will make a massive difference to your organization, the protection of valuable data and its overall security posture. But don't expect everyone to be as excited when you turn the data classification solution switch 'on'.
Think about it from the user's viewpoint: what's in it for them? How does classification help them do their jobs? Will it make their lives easier?

Few users love extra process, so show them that applying data classification is simple, fast, and reliable. Give real-life scenarios to help users relate the new solution to their daily work. Show them how systems work around the classifications they've applied. Make sure they know the new system will make their jobs easier, and show them the reverse too. Highlight that thinking about each piece of information when handling it is insignificant compared to the consequences and embarrassment of unwittingly sharing sensitive information. See our "Why classify" short video as an example of socializing your classification initiative.

5. Allowing exceptions

A data classification system must be supported and used from the top down. Any exceptions place the whole initiative at risk, practically and for widespread acceptance and use. Make sure you have management buy-in, in theory and in practice.

Some organizations expect the Executive Assistant teams to apply data classification and exclude the senior executives. This situation is high-risk, as senior leaders often generate the most sensitive organizational information.

Applying labels to protect sensitive information affects everyone, so everyone must be involved. No exceptions.

6. No policies

Clear, accessible, published data classification policies and guidelines are a powerful resource to help your teams recognize sensitive information, apply appropriate markings, and handle data correctly. A concise, practical policy manual improves user productivity because they know what to do with sensitive data and exceptions, reduces the risk of information mismanagement, and strengthens your organization's overall security posture.

7. Using default classifications

Default classifications occur when organizations promote a 'standard classification', instead of personally assigning a classification. Problems arise with system-generated classifications because almost all users tend to use the default without question. After all, it is easy, fast, and takes no thought. Ironically, this is the opposite of the desired outcome, which is for every user to *think* about information every time they handle it. Widespread use of default classifications usually indicates the classification framework has yet to be defined clearly.

8. Insufficient support

The most effective data classification schema presentations are simple, intuitive to select, and achieve the organization's needs for distinct markings. Questions arise with any software, and it is crucial answers are readily available, easily understood, and quick to follow. Any complex, time-consuming selection turns users off and stops the desired classification behaviors. Janusnet recommends a discreet, brief pop-up helper for each classification to give users real-time help.

9. Lack of infrastructure integration

The most robust data classification solutions ensure teams mark information files with visible classifications and tag the file's metadata with a matching classification. Visual markings remind users how to handle information. Metadata markings enable integration with downstream systems, such as email gateways, Data Loss Prevention (DLP) tools, security solutions, and operating systems, to ensure automated, consistent information control. Such integration is invaluable because users are fallible and make mistakes. Automated actions include alerts for incorrect classification, blocks on sensitive information sent externally by email, and insights into classification usage trends. The combination of manual and metadata data classification delivers a robust, cost-effective information protection program. Integrated data classification solutions help create a solid foundation for Zero Trust frameworks. Learn more here.

10. Not knowing what to measure

Measuring the metrics that matter to your organization is essential across all operational areas, including data classification. From the outset of your program, be clear on what you want or need to know and aim to use existing data sources to deliver the necessary insights. A little planning goes a long way.

For example, do you want to know when someone downgrades a classification or skips applying one? Do you need to know how much of your organization's data is truly sensitive? Do you want to track how much data classification usage changes over time or how well users are adopting a new schema? What forensics will your risk management team request in the event of a data breach?

11. Too much, too soon

The Pareto Principle (more commonly known as the 80/20 rule) applies to many areas of work and life, and data classification is no exception. It's tempting, but sometimes overwhelming, to classify all data from Day One. The good news is that isn't necessary. Instead, prioritize the areas of data classification with the most significant impact on your organisation. Then move sequentially through each priority area to progressively improve the overall security posture.

For example, if preventing data loss is the first priority, focus on the most likely vulnerability point (email). Data classification never has to be all or nothing. Keep it simple, start small, expand thoughtfully, and your data classification practice will be successful, accepted, and deliver the outcomes your organization needs.

About Janusnet

Janusnet is a pure-play, global leader in data classification trusted by governments and commercial enterprises worldwide to reduce the risk of data loss and improve information handling. Janusnet is renowned for its software's reliability, functionality, and ease of use, backed by a highly responsive development and support team.

Getting started

For more information and to get started with comprehensive data classification solutions that meet compliance requirements and protect your organization's data, visit https://www.janusnet.com/what-we-do

Or contact us for a chat:
t: Americas: +1 571 577 8004
Asia Pacific: +61 2 8004 9300
Europe: +44 20 3318 0785
e: info@janusnet.com