HOW TO CREATE

The Perfect Data Classification Policy

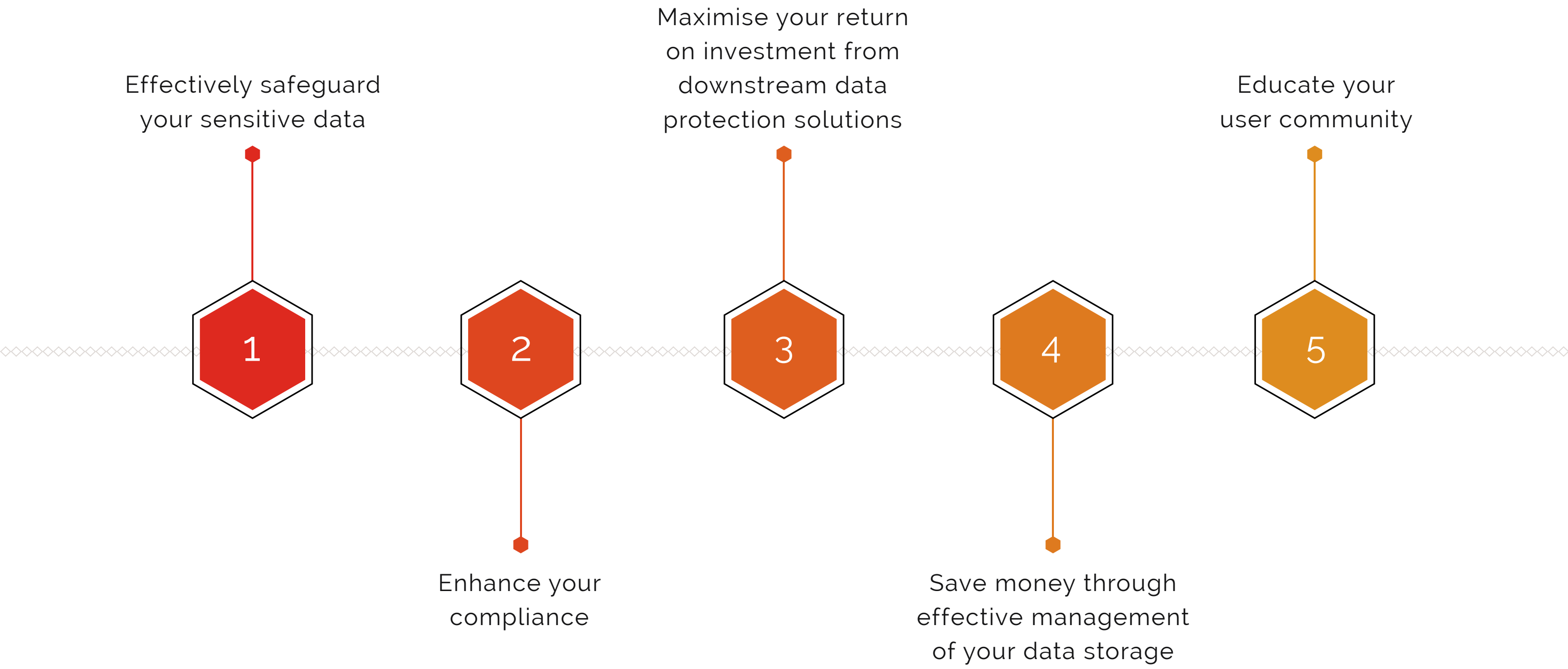
A REPORT BY

HANDD
BUSINESS SOLUTIONS

Enquiries: +44 (0)8456 434 063
www.dataclassification.com
www.handd.co.uk

INTRODUCTION

You've taken the plunge and decided to deploy a data classification solution. Now, you need to develop a data classification policy that will help you get the most from your investment - one that will support you to:



1. Effectively safeguard your sensitive data
2. Enhance your compliance
3. Maximise your return on investment from downstream data protection solutions
4. Save money through effective management of your data storage
5. Educate your user community

What is a data classification policy and why is it important?

A data classification policy helps you to identify critical and sensitive data.

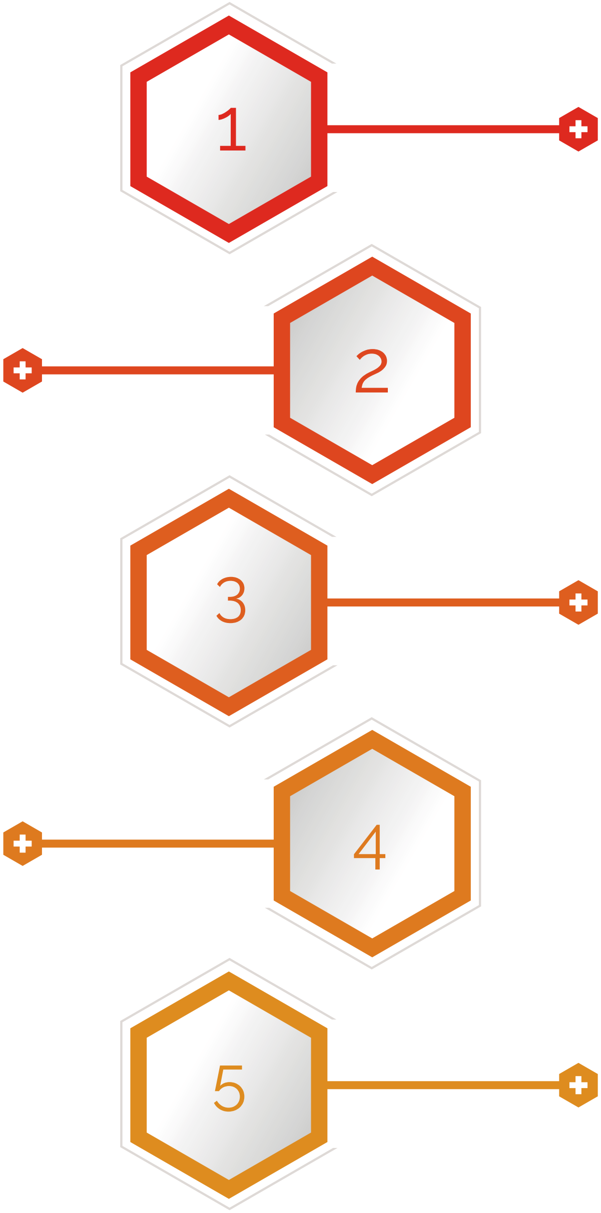
It shouldn't be limited to defining the categories used to label the data and indicating which categorisation each data file belongs to. Your data classification policy should provide granular instruction on how data should be handled throughout its lifecycle.

Your data classification policy should serve as a reference guide on how you will use visual markings, metadata and handling rules to help you meet each of the 5 steps in protecting your critical data.

DATA CLASSIFICATION

FIVE STEPS TO PROTECT YOUR CRITICAL DATA

By ensuring that your data classification policy covers each of these elements, you'll be able to maximise the effectiveness of data protection within your organisation. Your data classification policy should determine:



HOW YOU WILL IDENTIFY DATA

What labels will you use to identify data to be protected?

DISCOVERING YOUR DATA

How and where should each class of data be stored and who should have access to it?

HOW YOU WILL CLASSIFY DATA

...and how each data file should be handled.

HOW YOU WILL SECURE DATA

...by using classifications to drive downstream technologies to protect your data.

HOW YOU WILL MONITOR YOUR DATA

What classifications will you monitor and how? Will you rely on alerts or manage regular audits?

Want to know more?

Speak to one of our independent data classification specialists
on +44 (0)8456 434 063 or drop us a line at info@handd.co.uk

www.dataclassification.com

CREATING A CULTURE OF DATA SECURITY

A data classification policy should provide a framework on which your organisation can nurture a culture of data security and develop healthy data hygiene habits in users.

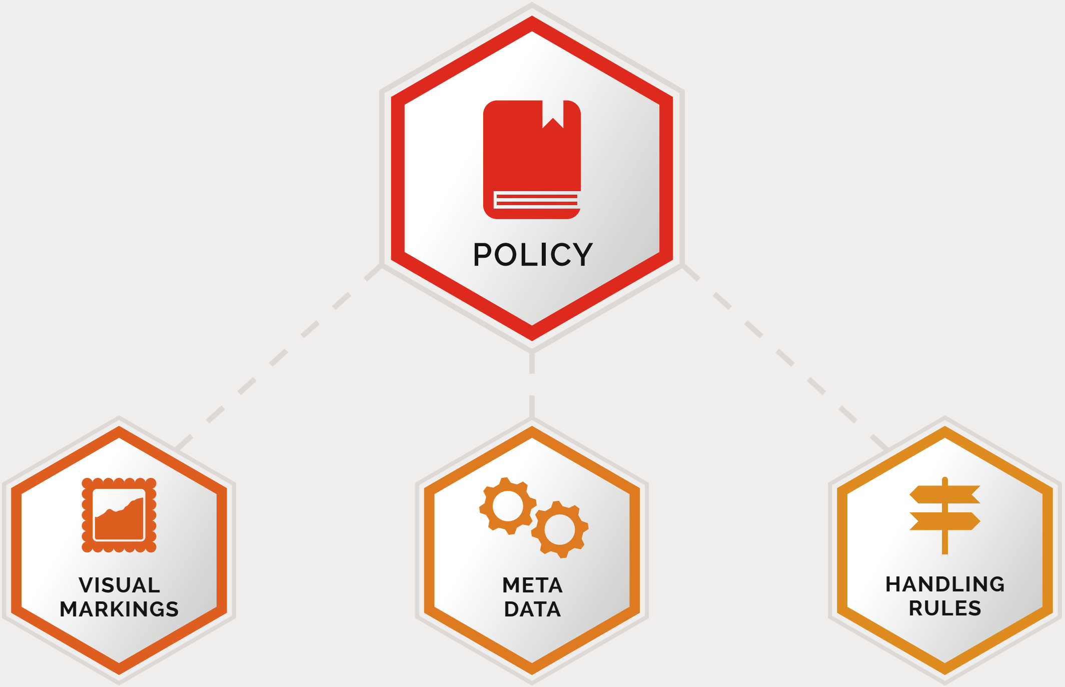
Continually requiring users to make decisions on the value of data makes data security an obligatory part of every user's workflow. The importance and sensitivity of data files becomes second nature through habit, shaping the way in which your employees handle, share and manage data.

Creating and encouraging a culture of data protection means users are less likely to leave data in public places. Chances are, they'll even think twice before sending documents outside of the company or mindlessly forwarding email chains.

The benefits of a culture of data security will extend well beyond inadvertent data loss.

A general awareness of the value of data will also make users wiser to phishing attacks or malicious software.

The 3 elements of a data classification policy:



Visual markings of each document's classification level provide increased awareness and reduce the chances of human error

The data behind the document, meta data, is added to each file to dictate how it should be treated and governed

Handling rules determine how each document is handled, including who can access, send and receive sensitive files and docs

Want to know more?

Speak to one of our independent data classification specialists on +44 (0)8456 434 063 or drop us a line at info@handd.co.uk

www.dataclassification.com

1 VISUAL MARKINGS

DATA CLASSIFICATION

As well as dictating the classification labels to be applied, your data classification policy should specify how visual markings should communicate the classification itself to the end user.

In addition to embedding the classification in the header or footer of a document, you could choose to feature the classification as a watermark, unmissable by anyone who happens to be looking at the document.

Visual markings serve to deter users from leaving documents on printers, photocopiers, desks or screens and can significantly reduce the opportunity for human error by:

- Increasing the awareness of the data user to the sensitivity of the document.
- Improving the awareness of data protection within the organisation by reminding users of the value of data.

2 META DATA

When data is classified, metadata is added to the file dictating how that file should be treated.

According to a survey carried out by Ponemon into 874 companies that had experienced a significant data loss event in 2016, internal access is to blame for 68% of data leaks. This startling figure highlights how working on a need-to-know basis is the best practical way to protect data.

Your data classification policy should define exactly what information is to be added to the metadata. It should provide granular details of:

- Where each classification of document should be stored
- Those allowed to access sensitive data

This level of governance means that your organisation can genuinely operate on a need-to-access basis, so the mail room staff can't access market-sensitive prototypes and your design team can't see employees' salary details.

The benefits of metadata

Metadata can be read by software. This means it can automate a response from your third-party data protection solutions, enhancing their reliability and improving your return on investment.

Metadata can make data files easier to recall and delete. It can even determine whether files are sufficiently sensitive to warrant being saved in your costlier (but more secure) on-site servers, or whether they can chance public cloud-based servers.

What else can data classification metadata drive?

- DLP solutions
- Event monitoring software
- Data governance
- Access control
- Retention policies and more

3 HANDLING RULES

Handling rules make up an important component of any effective data classification policy.

These handling rules determine how documents within each classification are to be managed and handled. They answer questions such as:

- Who can send, access and receive sensitive data?
- Should a user be alerted if they are attempting to send sensitive data to an unauthorised recipient?
- Should a user be challenged or follow a confirmation process before being able to send sensitive data?
- What happens when an employee tries to send data to an unauthorised third party?
- And should the data be stopped in its tracks?
- Should management receive visibility on the attempt in a report?
- And when should interventions or alerts occur

Your complete data classification policy should combine a number of these measures to:

1) Deliver a comprehensive data protection road map

2) Determine whether classification is mandatory and provide intuitive feedback and guidance to the user community

3) Provide guidance on how preventative measures are implemented to stop breaches and misuse from occurring at the point the data is created.

In achieving this your data classification policy will play an important ongoing role in developing a culture of data protection and enhancing the way in which you protect your data.

ABOUT HANDD

HANDD Business Solutions are specialists in delivering data classification projects. HANDD have deployed data protection solutions in 25 countries around the world, helping to safeguard critical data for 8 of the World's largest banks and 45% of the FTSE 100.

Find out how HANDD can help you protect your data.

HANDD
BUSINESS SOLUTIONS

Want to know more?

Speak to one of our independent data classification specialists
on +44 (0)8456 434 063 or drop us a line at info@handd.co.uk

www.dataclassification.com