JUTA
POPIA PORTAL

ISSUE NO 16 • ISM TIPS FOR SMEs – BYTE 4 • JANUARY 2023

IsM | (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 4

Disclaimer: We are not 'information security management' experts by any stretch of the imagination. This article includes purely practical recommendations on ISM tips which we have found helpful for smaller organisations which we have assisted with POPIA compliance issues.

Photo: Tayeb Mezhadia Pixabay

1. OVERVIEW

In our fourth byte, we will further break down the first policy statement that a basic ISM policy should include – classifying your information. We will also discuss how to implement this policy statement within an SME environment with limited time and resources.

2. WHAT DOES ‘CLASSIFYING’ YOUR INFORMATION EVEN MEAN?

Photo: stock.adobe.com

Information classification’ is a central concept in ISM and is a process during which an organisation assesses the information they hold and the level of protection it should be given. Organisations usually only classify information in terms of confidentiality, but in Chapter 3, we recommend that you should add classifications of personal information to this for POPIA compliance purposes. Here are the examples of different classes of information we suggest having:

- public information;
- private information;
- confidential information;
- personal information; and
- special personal information.

3. WHY SHOULD YOU CLASSIFY YOUR INFORMATION?

Identifying your information according to a certain classification ensures that the information receives the appropriate level of protection according to its importance to your organisation. The classification process also assists with applying a risk-based approach to your POPIA compliance because it highlights the most critical areas to concentrate your time and resources on from an ISM perspective. Classifying information also helps implement internal access control procedures and determine which employee levels have access to which type of information.

Photo: Stephan Pixabay

Photo: Gerd Altmann Pixabay

4. HOW DO YOU CLASSIFY YOUR INFORMATION?

So how do you implement this policy statement within your organisation? Overall we recommend following a four-step process based on the requirements set out in the ISO 27001 and 27002 standards. You can get a more comprehensive overview of this four-step process in this blog.

4.1. STEP 1 – *Compile an information asset register*

What is an information asset register? The simplest definition is an inventory that lists the assets, systems and applications you use to process or store information and records within your organisation.

What is an information asset? The UK National Archives defines an information asset as a 'body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively'. For example, an employee file that HR holds is an information asset containing different personal information and records of an employee that are grouped together. A direct marketing database comprised of many contacts is another example of an information asset.

Typically, information asset registers will list what type of information the information asset is (public, private, personal etc), who the information asset owner is and the relevant retention period.

Good resources to use for compiling your information asset register are:

- ICO and UK National Archives – a great guide on how to identify information assets and how to compile your register;
- New Zealand Government – also a great guide on how to identify information assets and how to compile your register; and
- the UK's Education Authority has a nice, simple Information Asset Register template.

Compiling an information asset register as a process can be as granular or as bird's eye-view as you want it to be, and your organisation needs it to be. For smaller organisations, the time spent on the discovery process (so you know what information and records your organisation holds) will also be relevant for compiling your PAIA manual and your records retention schedule. You should be able to re-use your information asset register to complete these two documents.

4.2. STEP 2 – *Have a classification standard and classify your information according to this*

Your information classification standard is a document which sets out the different types of security classifications you have decided on for your organisation (e.g. public, private, confidential, personal). The document provides a definition and examples of each classification. This enables information asset owners to classify the information and records they are responsible for.

Good examples of information classification standards include:

- London School of Economics
- York University.

4.3. STEP 3 – *Have a labelling standard and physically label your information according to its classification*

This document sets out what information types need to be physically labelled (e.g. stamping a file as ‘confidential’) and advises on how to do this depending on what format the information is in (hard copy, electronic MS Word document, email etc). This is important because protective labelling assists organisations with better control over their information and can reduce security compromise risks because users know immediately how to treat the information or record. You can purchase highly advanced and expensive information labelling solutions, but there are also practical, simple ways to label your information and records.

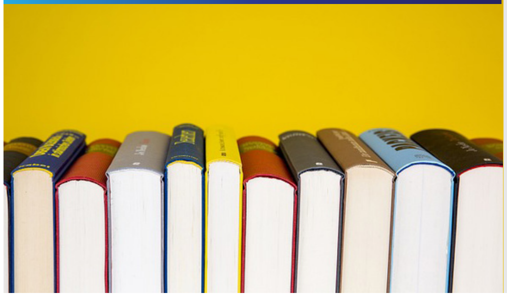
You can find nice examples of labelling standards that offer simple labelling solutions, which are very workable in smaller organisations, here, here and here.

4.4. STEP 4 – *Have a handling standard and create security rules about how to handle different types of information in different scenarios*

This document sets out physical security rules and controls for the different types of information. Different rules or controls will apply, depending on what scenario you are using that type of information within (e.g. granting internal access, sharing to an external party, storing, backing up etc) and what format that information is in (electronic versus hard copy). We will dive into information-handling rules and controls at a later stage, but here are some nice examples of information-handling schedules we have found:

- Derbyshire County Council
- York University
- New South Wales Government Department Guidelines.

5. FURTHER READING



- You can read more about ISM requirements generally in Chapter 5.
- You can read more about classifying and identifying the types of information your organisation holds in relation to compiling a records retention schedule in Step 11 of ‘Get Compliant’.
- You can read more about classifying and identifying the types of information your organisation holds in relation to compiling a PAIA manual in Step 8 of ‘Get Compliant’.

juta