JUTA
POPIA PORTAL

ISSUE NO 8 • ISM TIPS FOR SMEs – BYTE 2 • SEPTEMBER 2022

IsM | (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 2

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: Markus Winkler/Unsplash

1. OVERVIEW

In our next byte, we will discuss documenting the ISM technical and organisational measures you have implemented within your organisation. Remember the series of questions we asked last time (e.g. do you have a data breach response plan, do you have a business continuity plan in place, do you keep a reliable record of who has accessed personal information within your organisation and so forth)? Many organisations answer 'yes' to the majority of these questions. The problem is that while these organisations may do these things, they have NOT DOCUMENTED the fact that they do these things and how. And that is what we are discussing right now.

2. WHY YOU NEED TO WRITE STUFF DOWN

Photo: Unsplash

Most lawyers will always tell you to 'put it in writing' if you put an agreement in place. But many auditors will also tell you that your risk controls, procedures, safeguards, and in this case, ISM technical and organisation measures, must also be documented in writing. It is fine and well that you actually DO the things you should be doing from an ISM perspective, but it is also vitally important to physically document what you do.

Pros of documenting your information security procedures and controls include:

- Good for accountability and transparency – everyone knows who has to do what and when.
- Good for standardisation and knowledge management – there are fewer grey areas on exactly who has to do what and when, and key processes, procedures and controls are documented for future reference and training if key people leave.
- Good for operational efficiency and continuous improvement – a good place to improve what you do from an ISM perspective is to document what you do.
- Looks professional – documenting what you do shows you are thinking about your information security management risks and dealing with them strategically.
- And lastly … documentation enables you to bring the receipts! You have actual written proof, which you can show auditors, regulators, lawyers, business partners etc. that you don't operate blindly in the dark from an ISM perspective!

This is an excellent blog about why documenting processes and procedures matters specifically for ISM, and **this is a nice blog** about how to start documenting your processes.

3. WHAT NEXT?

Get started on that documentation! We suggest you start with a basic ISM Policy and go from there. The ICO (the UK's data protection regulator) has an **excellent resources page** specifically related to this topic. Additionally, this is an **excellent blog by Dataversity** about writing an information security policy. We also think this blog should give you a **good overview of the basics**. The Centre for Information Policy Leadership has also published a highly useful report called What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, which has a **section on ISM policies and procedures**. For a very comprehensive overview of ISM, look at the IAPP's resources **here**.

Additionally, you can read **Chapter 5** on Information Security Management. Looking at the ISM section of '**Step 2**' of 'Get Compliant' and '**Step 10**' of 'Get Compliant' should also help you. Lastly, look at the 'Information Security Management Policy' questions in '**Step 4**' of our 'PIIA like a Pro' Step-By-Step Guide.

juta