JUTA
POPIA PORTAL

ISSUE NO 24 • ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMES – BYTE 6 • MAY 2023

ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 6

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: Gerd Altmann from Pixabay

1. OVERVIEW

In our sixth byte, we will break down the third policy statement you should include in your basic ISM policy – taking appropriate, reasonable technical and organisational measures to protect the information within your possession or control.

2. WHAT ARE 'APPROPRIATE, REASONABLE TECHNICAL AND ORGANISATIONAL MEASURES'?

Section 19(1) of POPIA provides that responsible parties must take 'appropriate, reasonable technical and organisational measures' to protect the personal information within their possession or control. Technical measures can include adopting an ISM standard like ISO 27001, encrypting or anonymising personal information, or even just ensuring that personal information in hard copy format is stored in a locked cabinet. Organisational measures include policies, processes, controls, plans, assessments, contracts, training (more training!) and monitoring.

It is important to note that these measures must apply to personal information stored in electronic and hard copy formats. Different measures will apply at different times of the personal information's lifecycle. For example, you will take different applicable technical and organisational measures to keep your personal information secure when you are storing it versus when you are sending it or sharing it versus when you are destroying it or preserving it or backing it up.

3. WHAT TECHNICAL AND ORGANISATIONAL SECURITY SAFEGUARDS DO WE RECOMMEND?

Photo: Werner Moser from Pixabay

First off, we recommend implementing an information handling schedule. What is this, you ask? This is a document which prescribes the specific technical and organisational security safeguards you must take for information which belongs to a specific classification (e.g. public, private, confidential, personal), information format (e.g. electronic or hard copy) and how you are processing that information (e.g. storing, sending internally, sharing, preserving or destroying). You can find nice examples to base your information handling schedule off here, here and here.

Then, we recommend implementing these technical and organisational measures concerning the information's classification, format and processing activity:

Electronic personal information:

- Have user authentication mechanisms (e.g. username and password to log in) in place to access personal information stored electronically.
- Implement two-factor or multi-factor authentication where possible.
- Have an acceptable use/end-user policy.
- Implement a password standard.
- If you are storing it on a portable electronic device (e.g. laptop, tablet, phone, USB flash stick etc.), always have a screen lock where relevant, report any missing device to your organisation immediately and password protect or encrypt your documents, files or hard drive where possible.

Hard copy personal information:

- Keep it stored in a locked cabinet or room.
- Ensure you keep a record of who accesses hard copy records of personal information (e.g. sign out register or access card swiping etc).
- Have a clean desk policy.
- Be careful about printing personal information in your workspace and then letting it lie around – instead, print a cover page so no unintended data breaches occur!

Sending personal information electronically (e.g. via email, WhatsApp, or other electronic platforms):

- Double-check the recipients' names, always.
- BCC, don't CC, when emailing multiple recipients.
- When you are sharing personal or confidential information via email, don't include it in the body of the email Instead, include the personal or confidential information in a password-protected attachment.
- Do not share large batches of personal or confidential information over email. Please consider all alternative sharing platforms, such as Google Shared Drives, OneDrive, SharePoint or other platforms sanctioned by your organisation, first.
- If you have to share personal information via WhatsApp for work purposes, enable two-step verification for your WhatsApp profile and backup your WhatsApp messages.
- Conduct general cybersecurity and anti-phishing training for your employees – especially those with administrative positions who have access to a lot of personal information within your organisation (i.e. 'gatekeepers').

Destroying personal information:

- Keep a paper shredder in your offices if you store a lot of personal information in hard copy format.
- If you use a professional services provider to destroy personal information in hard copy format or, for example, to delete personal information stored on hard drives or old electronic devices, always use a reputable service provider, and get a certificate of destruction from them.

4. WHAT NEXT?

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.

Photo: Unsplash

juta