JUTA
POPIA PORTAL

ISSUE NO 3 • ISM TIPS FOR SMMEs – BYTE 1 • JULY 2022

IsM | (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMMEs – BYTE 1

Disclaimer: We are by no means '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.

1. OVERVIEW

Why ISM tips for SMMEs? We've been doing this for a while and have noticed that this is one area of POPIA compliance that smaller organisations battle with. Keeping any information continuously secure, addressing constantly evolving risks and reviewing the adequacy of internal controls in this area is a mouthful for any organisation (let alone a small one!). That is why we are starting this series, to break down this mouthful of a POPIA compliance area, one byte at a time 🙂

Photo: FLY:D/Unsplash

2. WHAT DOES POPIA ACTUALLY REQUIRE YOU TO DO TO KEEP PERSONAL INFORMATION SECURE?

POPIA does not require organisations to adopt any specific standard or technology for ISM purposes. Section 19(1) of POPIA prescribes 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 hardcopy format is stored in a locked cabinet. Organisational measures can include policies, processes, controls, plans, assessments, contracts, training (more training) and monitoring.

Section 19(2) of POPIA is a bit more specific and requires the responsible party's reasonable measures to:

- identify risks to personal information in the responsible party's possession or under the responsible party's control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are properly implemented; and
- regularly update safeguards in response to new risks or deficiencies in safeguards.

3. SO… HOW DO YOU WORK OUT IF YOUR **'TECHNICAL AND ORGANISATIONAL MEASURES'** ARE UP TO SCRATCH?

The first step in determining if your 'technical and organisational' security measures are considered 'reasonable' enough to meet POPIA standards is to do a bit of a (for lack of a better word) 'gap analysis'. We do this when we assist smaller organisations by asking their IT departments or IT personnel the following questions:

- Do you review the types of information security risks your organisation faces regularly?
- Do you check that your information security risk safeguards are correctly implemented regularly?
- Do you review the adequacy of your safeguards to protect your organisation against these information security risks regularly?
- Do you have a procedure in place to report and deal with a data breach (i.e. a 'data breach response plan')?
- Do you have a business continuity plan in place if, for example, you have a fire, flood, pandemic, electricity outage, fibre outage or other event, which means personal information within your possession or control is unavailable? What is your backup plan?
- Do you have a reliable record of all activities of all users who have accessed personal information at your organisation so you can detect unauthorised access or processing if it occurs? e.g. Do you keep access logs, and how far back do they go timewise?

4. WHAT NEXT?

We will keep going with this series on ISM tips for SMMEs in the next few newsletters. In the meantime, you can read Chapter 5 on Information Security Management. Looking at the ISM section of 'Step 2' 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