JUTA
POPIA PORTAL

ISSUE NO 12 • ISM TIPS FOR SMEs – BYTE 3 • NOVEMBER 2022

IsM | (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 3

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: Pixabay

1. OVERVIEW

In our third byte, we discuss what we would put in a basic Information Security Management ('ISM') Policy for an SME. This gives you a general idea of what policy statements and topics your ISM policy should adopt and address.

2. OUR *WHAT, WHERE, WHO* AND *WHY* FOR AN ISM POLICY

Photo: Unsplash

2.1. FIRSTLY, THE BARE ESSENTIALS FOR ANY POLICY

These are the bare essentials which any policy should contain:

- Purpose; Why do you need this policy? What are you aiming to achieve?
- Scope: Who, what, and where does this policy apply to? All information? Only electronic information? All employees? All independent contractors? Your South African office only? Your Southern African branches?
- Consequences for non-compliance with this policy: For your organisation? For your employees?
- Roles and responsibilities: Who is responsible for doing the thing? Zombies? Your information officer? Your IT department? Your employees?

2.2. WHAT POLICY STATEMENTS AND TOPICS YOUR ISM POLICY SHOULD COVER

- Classify information: You need to manage information security risks by classifying your information according to the level of risk your organisation would face if the confidentiality, integrity or availability of your information is compromised (for example, categories such as 'public', 'private', 'personal' and 'confidential').
- Access control: You need to ensure that roles-based access to information is implemented throughout your organisation. For example, only people who need access to information to do their jobs should have access. Access control also helps when you have a security breach because you know who is permitted to access the information and who is not.
- Appropriate, reasonable, technical and organisational measures to protect the information within your possession or control: You must implement appropriate, technical and organisational measures to physically keep your information secure. For example, your ISM policy is an organisational measure. Keeping all paper documents containing personal or confidential information in locked cabinets is an example of a technical measure.
- Information quality: You need to ensure that your organisation's personal information is 'complete, accurate, not misleading and updated where necessary'. You need to put procedures in place to ensure this.
- Information availability and business continuity: You need to ensure that information is backed up and contingency plans are in place, for example, if a power outage, cybersecurity attack, fire, flood or pandemic occurs etc. You need to have a business continuity plan in place to ensure the availability of your information when disaster strikes.

Photo: Scott Graham Unsplash

- Manage third parties: You need to manage all third parties (external organisations and persons) with whom you share information or grant access to your information to. This relates to how you share or grant access to the information, what contracts you have in place and how you keep tabs on which external organisations you share information with or grant access to your information (for example, a contract register). Third party risk management also helps when you have a security breach because you know who is permitted to access the information and who is not.
- Manage and respond to security compromises: You must have a procedure where people can report data breaches and a basic response plan in place.
- Conduct information security risk assessments: Document how and when you assess and re-assess the type of information security risks your organisation faces, risk severity, what safeguards you have in place to protect against these risks, whether these safeguards are being implemented properly as well as the actual ongoing adequacy of these safeguards to guard against potential information security risks. Also, when, for example, you need to conduct a Personal Information Impact Assessment, this information security risk assessment will form part of that assessment as the security compliance component.

3. WHAT NEXT?

Get started on that policy drafting! We suggest you start with a basic ISM Policy outlined above and go from there!

Additionally, you can read **Chapter 5** on Information Security Management, which covers topics like security compromises and response, managing information security risks in general and information availability. You can read about information quality in **Chapter 9** and you can read about managing third parties in Step 6 of 'Get Compliant'. You can read more about ISM policies and other policies in general in **Sections 20.2.5** and **20.2.6** of **Chapter 20**. 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. These are the questions you can ask as part of an information security risk assessment of a process.

juta