JUTA
POPIA PORTAL

ISSUE NO 28 • ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMES – BYTE 7 • MARCH 2024

ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 7

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: Pexels - Cottonbro

1. OVERVIEW

In our seventh byte, we will break down the next policy statement you should include in your basic ISM policy – information availability. That is, you must ensure that you backed up your information and have contingency plans to restore your information's availability when disaster strikes.

2. WHAT EXACTLY IS 'INFORMATION AVAILABILITY'?

Availability' comprises the 'A' portion of the 'CIA' Triad regarding information security management. NIST defines 'information availability' as 'ensuring timely and reliable access to and use of information' or as 'the timely, reliable access to data and information services for authorised users'.

3. WHAT DOES POPIA REQUIRE?

POPIA does not have explicit requirements regarding the availability of personal information. However, section 19(1) of POPIA requires responsible parties to take security measures to prevent the loss or unauthorised destruction of personal information. Therefore, from this, you can gauge that responsible parties are responsible for ensuring the following in respect of personal information within their control:

- that it is not lost; and
- that authorised users have timely and reliable access to this personal information.

4. WHAT DOES THE GDPR REQUIRE?

Photo: Pexels

The GDPR is a bit more explicit regarding what it requires in terms of information availability and can offer you a further understanding of this requirement. Article 32(1)(c) of the GDPR states:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate – the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.*

The UK Information Regulator, the ICO, offers a bit more insight into this requirement by stating:

> *The UK GDPR does not define what a 'timely manner' should be. This therefore depends on:*
>
> - *who you are;*
> - *what systems you have; and*
> - *the risk that may be posed to individuals if the personal data you process is unavailable for a period of time.*
>
> *The key point is that you have taken this into account during your information risk assessment and selection of security measures. For example, by ensuring that you have an appropriate backup process in place you will have some level of assurance that if your systems do suffer a physical or technical incident you can restore them, and therefore the personal data they hold, as soon as reasonably possible.*

This requirement adds a new layer to the meaning of 'information availability'. This requirement goes a bit beyond ensuring personal information is not lost and is accessible in a timely and reliable manner in general. Suppose access is lost due to a physical or technical incident (e.g. a power outage, cybersecurity attack, fire, flood or pandemic). In that case, you can restore availability in a timely and reliable way.

5. HOW DO YOU ENSURE THE AVAILABILITY OF YOUR INFORMATION PRACTICALLY?

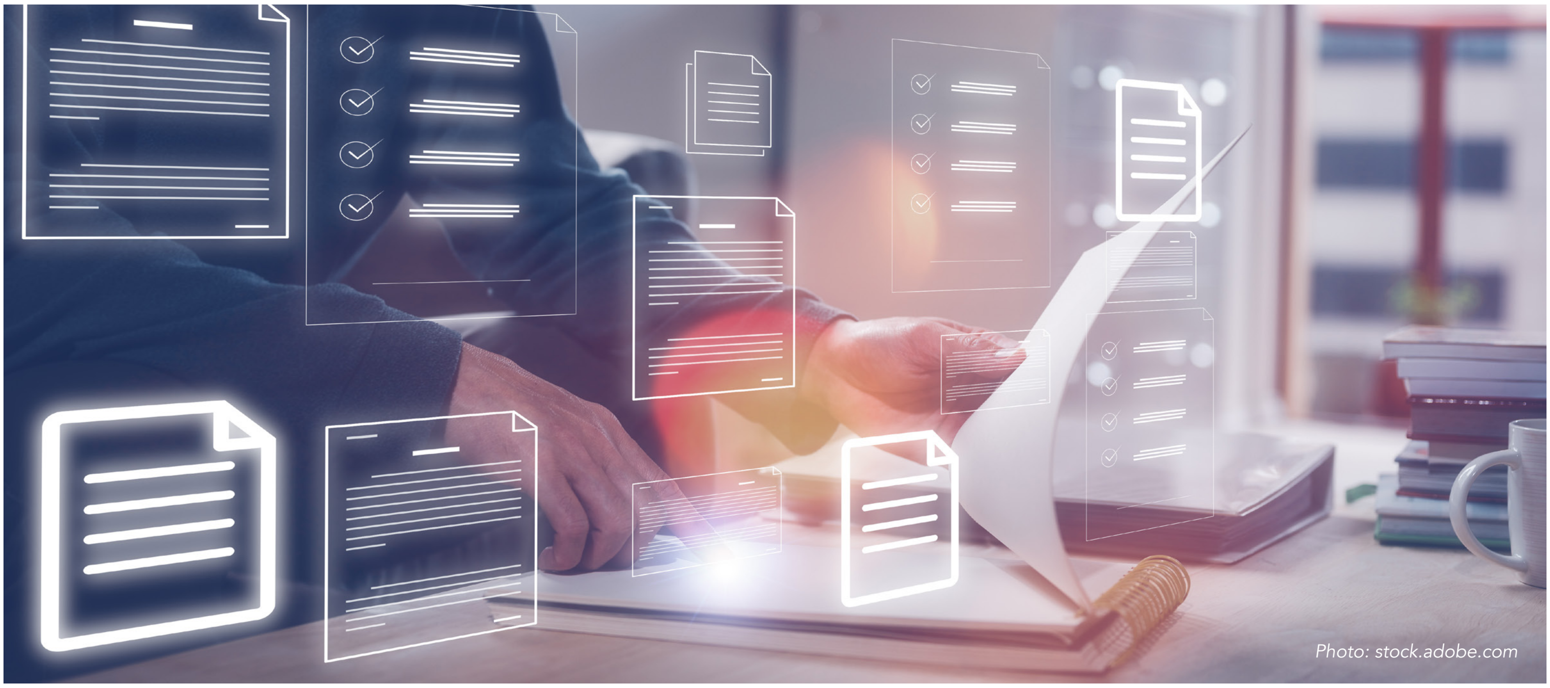

Photo: stock.adobe.com

From a practical perspective, you can ensure that you have documented business continuity management and disaster recovery plans and procedures in place to ensure the availability of your information when disaster strikes. Again, we are not ISM experts, so our role is to only point you in the direction concerning the technical side of things. Here are some resources explaining the basics of business continuity management and disaster recovery.

6. 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: iStock