JUTA
POPIA PORTAL

ISSUE NO 20 • ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMES – BYTE 5 • MARCH 2023

ISM (INFORMATION SECURITY MANAGEMENT) TIPS FOR SMEs – BYTE 5

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: Cottonbro/Pexels

1. OVERVIEW

In our fifth byte, we will further break down the second policy statement a basic ISM policy should include – access control. We will also discuss what implementing this policy statement entails and tips for doing so within an SME environment with limited time and resources.

2. WHAT IS 'ACCESS CONTROL'?

We scoured the internet for some definitions, and we think Microsoft says it best with this definition:

> ***'Access control is an essential element of security that determines who is allowed to access certain data, apps, and resources—and in what circumstances. In the same way that keys and pre-approved guest lists protect physical spaces, access control policies protect digital spaces. In other words, they let the right people in and keep the wrong people out.'***

It is important to note that your access control processes can limit a user's access virtually (e.g. to electronic information, computer networks and applications) and physically (e.g. to certain buildings, safes or storage facilities). Overall, access control processes ensure that a user is granted the appropriate permissions based on a predefined set of rules.

3. WHY IS IT SO IMPORTANT?

Photo: stock.adobe.com

Access control is essential for protecting the security of your organisation's personal and confidential information from external and insider security threats. For example, the Ponemon Institute revealed in their 2022 **'Cost of Insider Threats' Global Report** that insider threat incidents have risen by 44% over the past two years, with over 50% of incidents being related to negligence. This means that it is not primarily malicious or criminal insiders causing data breaches, but regular employees making mistakes. This shows just how important it is, from an information security management perspective, to ensure that your internal access control is managed carefully according to predefined rules.

4. GUIDANCE ON ACCESS CONTROL RULES

Based on our experience, these are the issues and components we think you need to address in the rules you set for managing access control within your organisation.

4.1. ROLES-BASED ACCESS (ACCESS ON A 'NEED-TO-KNOW' BASIS)

We suggest you adopt a roles-based model of access control. There are **other models** but opting for a roles-based model means that users are granted access based on what information they need to do their job or perform their roles. A user's level of access is not based on how senior they are or how long they have worked for your organisation, for example.

4.2. LEAST PRIVILEGE (ACCESS ON A 'NEED-TO-USE' BASIS)

We suggest you adopt the least privilege principle when granting users access. Least privilege means that you are granting the user the minimum levels of access or permissions to users which are needed to perform their job or function. For example, an HR assistant may have viewing rights to employees' electronic profiles but does not have editing rights to change any information on those profiles. On the other hand, the HR manager will have both viewing and editing rights.

4.3. USER REGISTRATION, MODIFICATION AND DE-REGISTRATION PROCESSES

We suggest you document and implement formal processes for user registration, modification and de-registration concerning access rights. This will ensure that you have an audit trail of the access rights a user has when they are first granted, change positions or leave your organisation's employment. This will also ensure that users' access rights are formally modified, suspended or terminated accordingly when they change roles or leave your employment. Administrators or gatekeepers in charge of authorising, modifying or revoking user access rights and permissions should keep a record of each decision they make.

Photo: Pexels

4.4. REVIEW OF USER ACCESS RIGHTS

We suggest you implement a formal process for reviewing user access rights and permissions within a specific period (e.g. on an annual basis). This will ensure that the user's access rights and permissions are appropriate for the user's current role. This prevents problems like '**privilege creep**' from occurring when users have access rights and permissions over and above what is appropriate for their current role. Privilege creep has been responsible for several costly data breaches globally, examples of which you can read about **here**.

4.5. PRIVILEGED USERS

Most organisations have users with elevated access rights and permissions to information, systems or facilities and are authorised to perform certain functions. These are referred to as 'privileged users' or 'super users' instead of 'standard users'. We recommend documenting the 'privileged users' versus the 'standard users' and applying different rules for privileged users. This is extremely important because privileged user account credentials or access mechanisms are the ones most often targeted by cybercriminals, and if they are compromised can cause the most damage.

These rules may include the following:

- Privileged user accounts should not be used for day-to-day purposes (e.g. email, web browsing etc.), and a privileged user should have a separate standard user account to use for these purposes.
- A privileged user account's access rights and permissions should be reviewed more regularly than a standard user.
- Implement more stringent authentication and security mechanisms to gain access to privileged user accounts.

4.6. ACTIVITY LOGGING AND MONITORING

We recommend monitoring and logging user account names and activities when users access information, systems or facilities to which they have been granted access rights and permissions. For example, keeping an activity log of who accessed what and when can take the form of system activity logs or a register for physical facilities. In case a data or confidentiality breach occurs, you must keep access logs of who has accessed personal and confidential information and when. Otherwise, it will be difficult to determine who is responsible for unauthorised access, use or disclosures.

5. FURTHER READING

- You can read more about ISM requirements generally in **Chapter 5.**

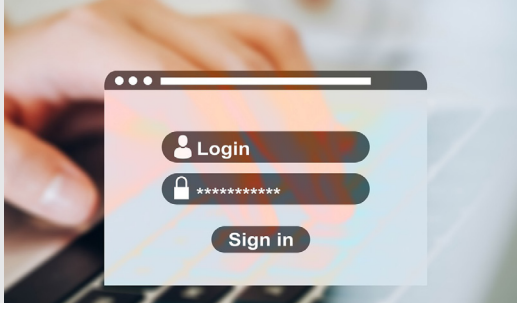

Photo: Unsplash

juta