JUTA
POPIA PORTAL

ISSUE NO 52 • POPIA AWARENESS TRAINING LEVEL 3 • MARCH 2025

POPIA AWARENESS TRAINING LEVEL 3

1. OVERVIEW

This is the third instalment of our POPIA Awareness Training for Employees series. We cover the basic requirements for securing electronic and physical personal information records.

Photo: iStock

2. SECURING PHYSICAL RECORDS

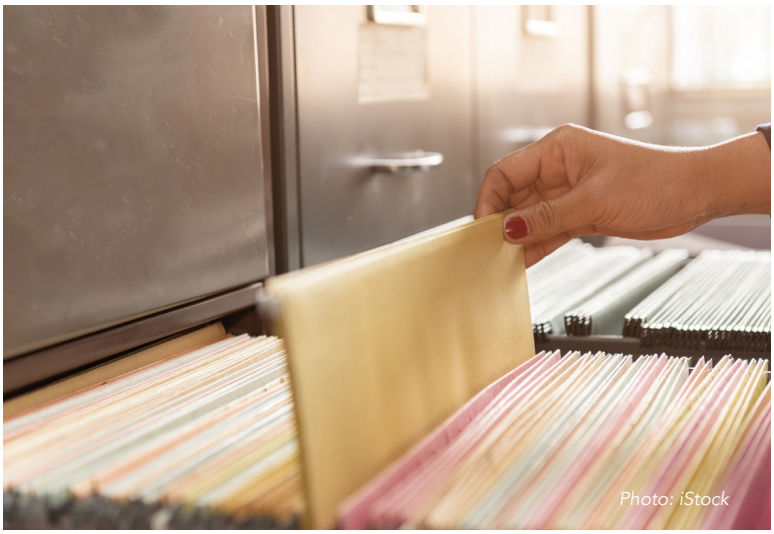

Photo: iStock

POPIA requires that we keep personal information secure from unauthorised access, use and loss. This means we must keep track of paper forms and documents and ensure that the wrong people don't read, copy or destroy them.

Here are a few security improvements all employees can make:

- **Shred what you don't need.** If you don't have a shredder, buy one or hire a shredding service.
- **Lock it.** Lock your filing cabinets, drawers and offices when not actively in use. Even when you go to the bathroom.
- **Restrict access**. Don't let just anybody into your administrative area. Ensure that only those who really need access to files or accounts have it. Don't allow any outsiders 'behind the counter'.
- **Clean desk policy.** Keep your appointment book, client files and accounts out of the public eye.
- **Keep it confidential.** Don't discuss customer details in person or on the phone in an area where others can overhear.

Implement these measures with your employees over the next few weeks and make sure you tick them all off the list.


Photo: iStock

3. KEEPING ELECTRONIC RECORDS SECURE

According to the latest research, 74% of data breaches are caused by human error. You should cover things like password requirements, access control and device management in your Information Security policies and procedures, but here are some easy and practical guidelines that everyone can follow:

- Don't include personal information in an email. If no alternative is available, attach a password-protected document rather than include it in the body. Instead, personal information records can be shared by other means, like a shared folder on Google Drive or SharePoint.
- Keep your computer and device up to date. Always install the latest updates as soon as possible – these updates usually include critical security patches.
- Don't write your passwords on a Post-it and keep it on your desk. Use a password manager to keep all your unique passwords safe.
- Everyone should check whether their email addresses and passwords have been compromised on https://haveibeenpwned.com/ and update any compromised passwords ASAP.
- Set your devices to lock automatically after 1 minute.

Here is a free phishing security test by KnowBe4. They have lots of free resources and training to get you started, check it out. You should do basic information security training with all staff at least once a year and record who completed it.

IMPORTANT: Ensure all employees know what a POPIA security compromise is and who to call if they suspect it. Remember that security compromises of personal information must be reported to the Information Regulator and data subjects must be notified. Read more here.

4. WHAT'S NEXT?

Read more about Information Security Management in Chapter 5 and POPIA training in Chapter 20. For practical advice on doing information security right, check out our ISM Bytes tips for SMEs.

Level 4 POPIA awareness training will focus on the POPIA requirements when you use service providers, known as operators, to process personal information on your behalf.

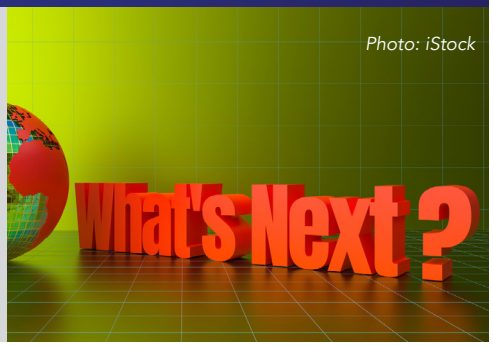

Photo: iStock

juta