JUTA
POPIA PORTAL

ISSUE NO 59 • POPIA AWARENESS TRAINING LEVEL 6 • SEPTEMBER 2025

POPIA AWARENESS TRAINING LEVEL 6

1. OVERVIEW

Welcome to the sixth instalment of our POPIA Awareness Training for employees. In this edition, we are focusing on what happens when personal information is accidentally (or intentionally) exposed, also known as an information security incident, a security compromise or a breach.

Photo: iStock

2. WHAT IS AN INFORMATION SECURITY INCIDENT?


Photo: iStock

An information security incident occurs when there are reasonable grounds to believe that personal information has been accessed or acquired by someone who should not have it.

This can include:

- A cyberattack or ransomware breach;
- The loss or theft of a device containing personal information;
- Sending an email with personal information to the wrong person; or
- An employee accessing records without permission.
- It does not matter whether the breach was accidental or intentional. If someone gains unauthorised access to personal information, it is a security compromise.

3. WHAT DOES POPIA REQUIRE YOU TO DO?

Photo: iStock

Under section 22 of POPIA, responsible parties must act quickly and transparently if an incident occurs. Here is a guideline on how to report a security compromise on the Information Regulator's eServices Portal.

A responsible party must:

- **Notify the Information Regulator** as soon as reasonably possible, ideally within 72 hours.
- **Notify the affected data subjects** unless their identities cannot be determined.

These notifications are not optional; they are legal obligations.

4. WHAT MUST BE IN THE NOTIFICATION?

When informing the affected data subjects, the notification must contain:

- What happened and what the potential consequences are;
- What steps you have taken or plan to take;
- What the individual can do to protect themselves (e.g. change passwords, monitor bank accounts); and
- If known, the identity of the person who accessed the information.

The goal is to help the data subject understand the risk and take action if needed, to protect their personal information from further risk and to limit the damage caused by the incident.

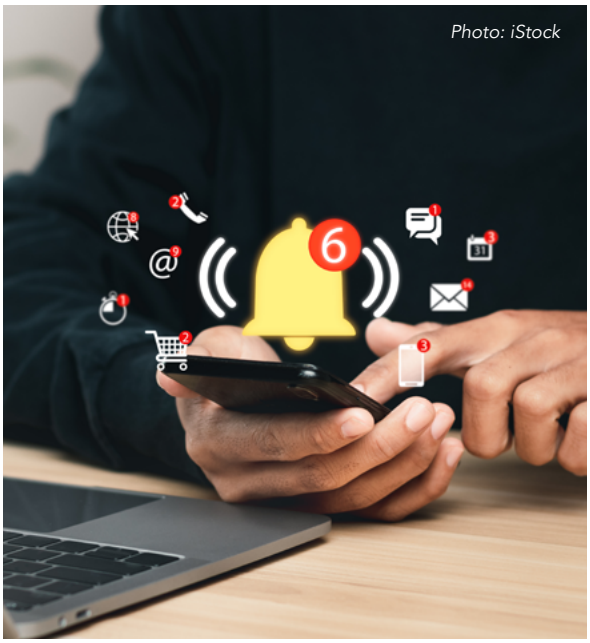

Photo: iStock

5. HOW TO PREVENT AN INFORMATION SECURITY INCIDENT

Photo: iStock

While this training focuses on response, the best defence is prevention. Here is how you can reduce the risk of a security compromise:

- Use strong passwords and multi-factor authentication;
- Do not leave laptops or files unattended;
- Be cautious when sending emails; always double-check recipients before hitting send; and
- Report anything suspicious to IT or your Information Officer immediately.

6. WANT TO READ MORE?

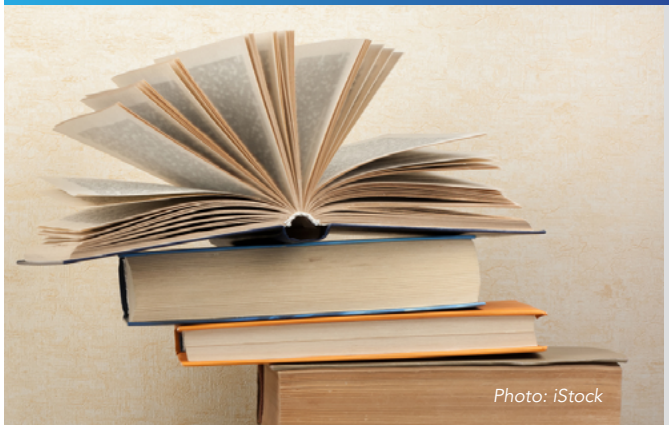
Photo: iStock

For more detailed guidance:

- Review Chapter 5 for everything about Information Security Management.
- See Chapter 5.6 for steps to take when an incident occurs.
- Check Chapter 19 for enforcement measures and penalties.

You can also find all required forms and instructions on the Information Regulator's website or eServices portal.

7. WHAT'S NEXT

Photo: iStock

Read more about Information Security Management in our *Ten Bytes on Information Security Management for SMEs*, available in the What's New archive section on the POPIA Portal.

In Level 7, we will discuss a data subject's rights and how to exercise those rights.

juta