BASIC INFORMATION SECURITY CHECKLIST FOR SMALL, LOW RISK BUSINESS OWNERS

FACT SHEET FOUR

This basic information security checklist has been developed to assist small, low risk business owners with POPIA compliance. The list is not exhaustive and each organisation's risk profile and exposure may vary. Organisations are encouraged to conduct a periodic risk assessment to determine whether a change in the risk profile requires additional safeguards to be implemented. Generally accepted information security standards and guidelines can be consulted for additional information.

□ Do you have a register (that records the information owner, storage locations and description) to record physical and electronic information assets? Information protection starts with a good understanding of the assets that are under the organisation's control, where personal information is accessed, shared and stored.

□ Are the roles and responsibilities with regards to information security defined and clearly communicated in the organisational policies and employment contracts? The responsibility and accountability for information security is a shared amongst all stakeholders in the organisation.

□ Do you continually educate your staff on the information security risks related to personal information protection? The human element of information security is often targeted by threat actors and is seen as one of the weakest links in the security chain. Regular security awareness sessions can be used to reinforce secure behaviour amongst staff members.

□ Do you have adequate physical security to protect your organisation's premises? Do you limit access to rooms and cabinets where physical records containing personal information are stored? How are your data centres physically secured (e.g. lock and key, biometric access, key card)? Personal information breaches are not limited to the electronic world, and physical loss or theft remains a risk.

□ Do you protect mobile devices containing personal information, including smartphones, tablets and laptops? Also consider that employee personal devices ("Bring your own device" or BYOD) are often used to access personal and other sensitive information.

□ Do your contracts with data operators (or key technology services providers) include the appropriate privacy clauses and require these third parties to implement information security controls to protect your assets?

□ Do you delete personal information after it is no longer necessary for the purpose of collection, and do you securely dispose of IT assets to ensure that personal information cannot be retrieved? Information stored on discarded data storage equipment (such as hard drives) that are not adequately cleared can often be recovered in a readable format using specialised software and equipment.

- □ Have you adequately backed-up your business critical information and does the process include at least one copy stored off site (not at the same premises as the live data) and offline (not network connected, for example on a backup tape)? The ability to recover backed up information within an acceptable timeframe is an important consideration and should be periodically tested.
- □ Do you have logical access controls, including strong passwords and multifactor authentication (MFA), to secure applications and services that store and process personal information? Passwords are often compromised during malicious privacy breaches and multifactor authentication is a proven mitigating factor.
- □ Have you secured your remote and cloud-based applications, including productivity and collaboration tools? Working from home has increased the potential for information security breaches. The responsibility to secure personal information stored and processed on cloud services remain with the responsible party.
- □ Have you implemented a securely configured firewall to protect your network from attacks originating from the internet? A firewall can be an effective network defence control and should be reviewed to ensure that the device has been appropriately configured.
- □ Have you securely configured your organisation’s Wi-Fi network? Secure protocols and complex passwords can be used to mitigate the threat of data interception over wireless networks.
- □ Have you implemented an anti-virus solution to identify and prevent malware from spreading on your network? Anti-malware can be effective in preventing malicious software on IT systems and should be consistently installed and updated.
- □ Have you secured your email solution to identify and prevent malicious email (including phishing, malware, fraud, etc.) and block it from reaching your organisation’s mailboxes? Preventing malicious email from reaching your staff mailboxes is an effective way to reduce threats.
- □ Do you regularly install patches and security updates on your IT systems including network infrastructure, mobile devices, operating systems and applications? Security incidents often occur as a result of outdated and vulnerable software platforms. Vulnerability assessments can be used to identify these issues and recommend solutions to address them.
- □ Do you use encryption technologies to protect the confidentiality of personal information on the systems and databases where it is stored, as well as in transmission? While encryption may not be able to prevent an information breach, it can protect the confidentiality of the information and the affected data subjects.
- □ Have you established an incident response process supported by a documented plan to effectively manage a privacy information breach (or other security incidents) in line with POPIA requirements? Despite implementing preventative measures, privacy incidents may still occur. An effective privacy incident response plan can help to minimise the impact while ensuring that your organisation conforms to POPIA regulations.