

The POPIA & Ransomware Risk Checklist

A 10-minute self-audit for South African businesses handling customer, client or employee personal information.

1 DATA PROTECTION & POPIA

- ☐ **We know exactly where customer and employee data is stored and who can access it.**
Unknown data flow = audit risk
- ☐ **We have a documented, tested breach-notification process.**
Required under POPIA
- ☐ **Personal information is encrypted both in transit and at rest.**
Unencrypted = direct violation
- ☐ **We produce regular (monthly/quarterly) compliance reporting.**
Most businesses produce none
- ☐ **Staff have received POPIA awareness training in the last 12 months.**
Human error is the #1 cause of breaches

2 COMMUNICATIONS & CALL SECURITY

- ☐ **Our phone calls are encrypted end-to-end (not just internet traffic).**
Legacy PBX = eavesdropping risk
- ☐ **Call recordings (if used) include POPIA-compliant consent prompts.**
Unconsented recording = violation
- ☐ **After-hours and overflow calls are routed reliably, every time.**
Gaps here = missed business
- ☐ **We can produce a full audit log of call activity on demand.**
Needed for compliance & dispute resolution

3 NETWORK & DEVICE SECURITY

- ☐ **IoT and connected devices (cameras, sensors, smart equipment) sit on an isolated network segment.**
Flat networks = single point of failure
 - ☐ **We have ransomware defence with automatic endpoint isolation.**
Not just antivirus
 - ☐ **We monitor the dark web for our business's leaked data or credentials.**
Most breaches are discovered too late
 - ☐ **We have a next-gen firewall with intrusion detection tuned to current threats.**
Generic firewalls miss targeted attacks
-

Why this matters

POPIA violations can carry fines of up to R10 million and criminal liability for directors. South Africa is among the most targeted countries in Africa for ransomware. Most businesses don't discover their exposure until something has already gone wrong.

How to use this

Tick every box that reflects your business today. Each unticked box is a potential exposure point. Score yourself at the end.

Your score

11-13 boxes ticked: Strong position. Worth a professional audit to confirm and document it.

6-10 boxes ticked: Meaningful gaps exist. These are exactly the gaps that turn into fines or downtime.

Below 6 boxes ticked: Significant exposure. We'd recommend a full risk assessment as a priority.

Want the professional version of this audit, free?

Book a free 30-minute POPIA & Cybersecurity Risk Assessment.

Innovo Networks (Pty) Ltd · Cape Town · Johannesburg · Durban · East London · Nairobi