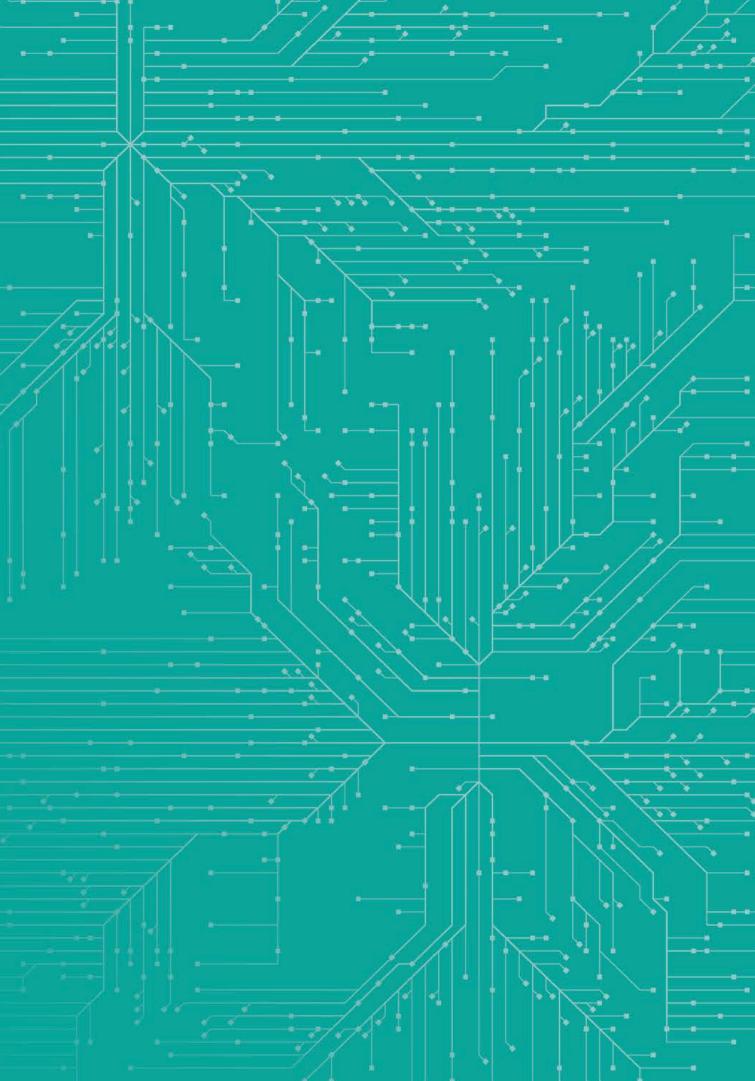


NETWORKS

Northbound Networks Cybersecurity Checklist



Protect your business year-round with these essential cybersecurity steps.



www.northbound.co.za

Update and patch systems

Keeping your software and systems up to date is the first line of defence against cyber threats.

- Regular Updates: Ensure that all applications, operating systems, and devices are running the latest versions. Many updates include crucial security patches that address newly discovered vulnerabilities.
- Automate Patches: Use automated patch management tools to streamline updates and reduce the risk of human error.
- Vendor-Supported Software: Avoid using outdated software that no longer receives security updates, as it creates an open door for attackers.

0 Z www.northbound

Strengthen access controls

Control who can access your systems and how they gain entry.

- Multi-Factor Authentication (MFA): Require a second verification method, such as a code sent to a mobile device, to log in.
- Least Privilege Principle: Grant users only the permissions necessary for their roles and responsibilities.
- Periodic Reviews: Regularly audit access permissions and deactivate accounts that are no longer in use to limit potential vulnerabilities.

0 Z northbound www.

Secure your data

Your data is one of your most valuable assets—protect it thoroughly.

- Encryption: Use strong encryption protocols for sensitive data stored on devices, servers, and during transmission.
- Regular Backups: Create daily or weekly backups of critical data and store them securely in off-site or cloud-based locations.
- Test your Backups: Periodically test your backups to ensure that you can recover data quickly in the event of an attack or failure.

ZO

northbound

www.

Protect your network

Prevent unauthorised access to your network and ensure smooth operations.

- Advanced Firewalls: Invest in enterprise-grade firewalls to filter traffic and block malicious requests.
- Intrusion Detection and Prevention: Deploy systems to monitor and react to suspicious activities in real time.
- Secured Wi-Fi Networks: Use strong encryption to protect wireless connections, and avoid using default network names and passwords.

0 Z northbound www.

Educate your employees

Your employees are often the first line of defence against cyber threats.

- Phishing Awareness: Train staff to recognise suspicious emails, links, and attachments.
- Best Practices: Educate employees on the importance of strong passwords, avoiding public Wi-Fi, and secure browsing practices.
- Incident Reporting: Create a clear process for reporting suspicious activity so threats can be addressed promptly.

ZO CO. www.northbound

Monitor and respond

Proactively monitor your network and have a plan in place for when something goes wrong.

- Real-Time Monitoring: Use advanced tools to detect unusual activity, such as multiple failed login attempts or large data transfers.
- Incident Response Plan: Document a step-by-step guide for handling breaches, including communication protocols and recovery steps.
- Security Logs: Regularly review logs to identify patterns and prevent future incidents.

DZ. CO. www.northbound.



NETWORKS

Contact us



087 743 2626 hello@northbound.co.za www.northbound.co.za

