NIKO Computers

Client IT Governance, Security and Staff Onboarding

Information Guide and Staff Acknowledgement

Document type	General information and staff acknowledgement only
Version	2.0
Effective date	25 June 2026
Client organisation	_____
Prepared by	NIKO Computers Pty Ltd

IMPORTANT INFORMATION NOTICE

This document is a general IT governance guide supplied to help a client communicate expected security practices to its staff. It is not legal advice, an employment contract, a managed-services agreement, or a guarantee that every cyber incident, policy breach, unauthorised activity or unlawful act will be detected or prevented.

The client remains responsible for its workplace policies, employee management, privacy notices, approvals and legal obligations. NIKO Computers only performs services that are expressly authorised by the client and included in the applicable written service agreement or approved support request.

1. Purpose of this guide

This guide helps business owners explain how company technology should be used and how IT and security requests should be handled when NIKO Computers is the appointed IT service provider.

- Reduce the risk of unauthorised software, applications and integrations.
- Clarify the responsibilities of the business owner, staff and NIKO Computers.
- Promote consistent approval, documentation and implementation of IT changes.
- Support safer onboarding, offboarding, access control and incident response.

2. Roles and decision-making

The business owner or authorised director remains the final business decision-maker. NIKO Computers provides technical advice and performs approved IT and cybersecurity work within the scope of the applicable service agreement.

Staff may request access, software, applications or configuration changes. They should not independently make tenant-wide, server, network or security changes unless the business owner has approved the request and NIKO Computers has completed the required technical and security review.

Nothing in this guide transfers ownership or control of the client's systems to NIKO Computers. NIKO Computers acts as an authorised service provider only.

3. Administrative and privileged access

Privileged access should be limited to the minimum level required for an approved task. Staff will not normally receive unrestricted administrative credentials, including:

- Microsoft 365 or Microsoft Entra Global Administrator access.

- Server, domain, firewall, router, backup or security-system administrator credentials.
- Passwords belonging to the business owner, another employee or a shared administrator account.

A request for elevated access may be considered where there is a documented business requirement, written approval from the client and an acceptable security risk. Approval is not automatic.

4. Software, cloud services and application requests

Before software, browser extensions, remote-access tools, cloud services or integrations are installed or authorised, the requester should provide enough information for a security and compatibility review.

- Application or software name, vendor and website.
- Business purpose and intended users.
- Required permissions and data access.
- Connections to Microsoft 365, email, SharePoint, OneDrive, Teams or other systems.
- Authentication requirements such as client secrets, API keys, certificates or service accounts.
- Licensing, implementation instructions, support contacts and whether the use is testing or production.

NIKO Computers may recommend approval, restrictions, an alternative product or rejection where the proposed solution creates unacceptable risk, requests excessive permissions, is unsupported, duplicates an existing system or conflicts with the client's environment. The final business decision remains with the authorised client representative, subject to technical and legal constraints.

5. Microsoft 365 and Microsoft Entra applications

Applications registered in Microsoft Entra may gain access to users, email, files, calendars, SharePoint, Teams and other business information. Staff should not independently perform the following tenant-level actions:

- Register enterprise applications or create app registrations.
- Create client secrets, certificates, federated credentials or service accounts.
- Grant tenant-wide consent or approve API permissions.
- Assign application roles or modify authentication, Conditional Access or security policies.

NIKO Computers can review and implement an approved application request after receiving complete technical details and written client approval. Credentials such as client secrets and API keys must be stored securely and should not be distributed through ordinary email or chat.

6. New staff onboarding

Before a new employee or contractor starts, the client should provide NIKO Computers with the person's name, role, start date, manager, licence requirements, required email and shared mailbox access, SharePoint and Teams access, software, network folders, remote access and any role-specific restrictions.

NIKO Computers will configure only the services included in the client's support arrangement or separately approved request. Access should be limited to what is reasonably required for the role.

7. Staff security expectations

Staff are expected to use company systems for authorised business purposes and to follow the client's policies. In particular, staff should:

- Protect passwords and multifactor authentication methods.

- Report suspicious messages, unexpected login prompts, lost devices and suspected incidents promptly.
- Request approval before installing software or connecting new services.
- Avoid bypassing security controls or removing antivirus, monitoring, backup or management tools.
- Avoid sharing accounts, moving company data to personal services or granting external access without approval.
- Return company equipment and assist with access removal when employment or engagement ends.

8. Monitoring, support and privacy

Where authorised by the client, permitted by law and included in the applicable service agreement, NIKO Computers may collect and review technical information needed to provide support and cybersecurity services. This may include device health, security alerts, malware events, patch status, backup status, login events, administrative changes, network events and other technical indicators.

This technical monitoring is intended for system administration, security, troubleshooting and incident response. It is not a promise of continuous employee surveillance, criminal investigation or detection of every inappropriate, unauthorised or unlawful activity.

The client is responsible for giving staff any workplace surveillance, privacy or acceptable-use notices required by law and for deciding how staff conduct will be managed. NIKO Computers does not make employment or disciplinary decisions.

9. Remote access and third-party vendors

Only remote-access methods approved by the client and NIKO Computers should be used. External vendors requesting access should identify themselves, explain the work, use time-limited access where practical and have access removed after the work is completed.

NIKO Computers may remove or restrict an unauthorised remote-access tool only where the client has authorised that action under the service agreement or support request, or where urgent temporary action is reasonably necessary to contain an immediate cybersecurity threat. The client will be notified as soon as practicable.

10. Staff departure and urgent security actions

The client should notify NIKO Computers as early as possible when a staff member or contractor is leaving or changing roles. Following authorised instructions, NIKO Computers may disable accounts, revoke sessions, reset passwords, remove MFA methods, transfer approved business data, remove application permissions and revoke remote access.

Urgent containment action may be taken only where authorised by the service agreement or where reasonably necessary to reduce an immediate threat. Any broader business, employment, legal or disciplinary decision remains the client's responsibility.

11. Requests, approvals and service scope

IT requests should be submitted through the approved NIKO Computers support channel. Requests involving elevated permissions, new applications or access to sensitive information may require written approval from the business owner or authorised manager.

A request is not approved until the authorised client representative and, where relevant, NIKO Computers have confirmed the implementation. Work outside the current service agreement may require a separate quotation or approval.

12. Responsibilities and limitations

This guide is intended to support good governance and reduce risk. It does not create a warranty or guarantee of uninterrupted systems, successful detection of all threats, prevention of all data loss, or compliance with every legal obligation.

The client remains responsible for business decisions, employee supervision, data ownership, lawful workplace monitoring, privacy notices, record retention and the selection of appropriate insurance and legal advice.

NIKO Computers' responsibilities are limited to the services expressly agreed in writing. Any responsibility or liability is governed by the applicable service agreement and Australian law, not by this information guide.

13. Contact

For software requests, access changes, technical support or security concerns:

NIKO Computers Pty Ltd
Email: support@nikocom.com.au
Phone: 1300 645 648 (NIKO IT)
Website: www.nikocom.com.au

Staff acknowledgement of receipt and understanding

This acknowledgement records that the employee or contractor received and understood the client's IT governance and security information. It is not an agreement between the individual and NIKO Computers, and it does not replace the client's employment agreement, workplace policies or legal obligations.

I confirm that I have read and understood this guide. I understand that software, applications, integrations, privileged access and significant IT changes must follow my employer's approved request and security process. I understand that technical system information may be monitored for authorised support and cybersecurity purposes, subject to the client's policies and applicable law.

Client organisation	
Employee/contractor name	
Position	
Signature	
Date	
Authorised manager	
Manager signature/date	

Client implementation note: The client should review this guide with its legal or HR adviser before adopting it as a workplace policy. The client should also ensure that any required privacy, workplace surveillance and employee consultation notices are issued separately.