DYNAMIC

ACCOUNTING - TAXATION - ADVISORS

Information Security Policy

Dynamic Taxation and Training Services

Purpose

Dynamic Taxation and Training Services is committed to protecting the confidentiality, integrity, and availability of client information and business data.

The purpose of this Information Security Policy is to establish the systems, procedures, and responsibilities required to safeguard information assets from unauthorised access, disclosure, modification, or loss.

This policy supports compliance with applicable laws, professional obligations, and best practice standards for accounting and taxation practices.

Scope

This policy applies to all employees, contractors, consultants, and third-party service providers who access or handle information belonging to Dynamic Taxation and Training Services.

It covers all information systems including:

- electronic data and databases
- client records and financial information
- physical documents and files
- communication systems including email and online portals
- cloud-based platforms and software systems.

Information Security Principles

Dynamic Taxation and Training Services adopts the following core information security principles:

- Client information must remain confidential.
- Information must be protected from unauthorised access or disclosure.
- Information systems must remain reliable and available to authorised users.
- Staff must follow secure practices when accessing, using, and sharing information.
- Security risks must be monitored and managed on an ongoing basis.

Information Security Controls

Confidentiality

All staff and contractors are required to maintain strict confidentiality of client information.

This includes:

- signing confidentiality agreements at the commencement of employment or engagement
- accessing only the information required to perform their duties
- always protecting sensitive client and financial information.

Confidential information must not be disclosed without proper authorisation.

Access Control

Access to information systems is restricted to authorised personnel only.

Security controls include:

- password-protected systems and user accounts
- access restrictions within internal databases
- permissions that limit staff access to information required for their role.
-

Passwords must not be shared with other individuals and must be maintained securely.

Physical Security

Dynamic Taxation and Training Services maintains secure premises to protect client information.

Security measures include:

- electronically secured premises accessible only to authorised staff using access cards
- designated client meeting rooms located outside secure work areas
- secure storage for physical documents and files.

Information Technology Security

The firm uses a range of technical controls to protect electronic information systems, including:

- secure servers and regularly updated technology systems
- firewall protection to prevent unauthorised network access
- ongoing system maintenance and software updates
- monitoring of systems to detect potential security vulnerabilities.

Secure Information Transfer

Sensitive information must be transferred securely when shared with clients or external parties.

Approved methods include:

- secure document portals or encrypted links
- protected folders for document exchange
- authorised communication platforms.

Staff must not transmit confidential information through unsecured channels.

Cloud-Based Systems

Dynamic Taxation and Training Services may utilise cloud-based software systems in order to provide efficient services to clients.

Where cloud services are used:

- reasonable steps are taken to ensure data security
- providers are selected based on their security standards
- information is handled in accordance with applicable privacy obligations.

Overseas Service Providers

In some circumstances information may be processed by overseas service providers where cloud-based platforms or technology services operate internationally.

Where personal information is disclosed overseas, Dynamic Taxation and Training Services takes reasonable steps to ensure the information is handled consistently with the **Australian Privacy Principles**.

Identity Verification and Fraud Prevention

The firm may collect identification information from clients to verify identity and prevent fraud.

These procedures support compliance with professional standards and regulatory obligations relating to identity verification and financial integrity.

Data Breach Management

Dynamic Taxation and Training Services complies with the **Notifiable Data Breaches Scheme** administered by the **Office of the Australian Information Commissioner**.

In the event of a suspected or confirmed data breach:

- the incident will be investigated promptly
- affected information systems will be secured
- impacted individuals will be notified where required
- corrective measures will be implemented to prevent recurrence.

All staff must report suspected security incidents immediately.

Staff Responsibilities

All staff and contractors must:

- follow information security procedures
- protect confidential client information
- report security risks or incidents immediately
- participate in relevant security training.

Failure to comply with this policy may result in disciplinary action.

Information Retention and Disposal

Client information is retained in accordance with professional and regulatory record-keeping obligations.

Where information is no longer required:

- electronic records will be securely deleted where appropriate
- physical documents will be disposed of using secure shredding services.

Monitoring and Review

Information security systems and procedures are reviewed periodically to ensure they remain effective and aligned with evolving risks and regulatory requirements.

Policy Review

This policy will be reviewed regularly and updated where necessary to reflect changes in technology, legislation, or business operations.

Last Updated:
13 February 2026