Consolidated IT Security Policy

VRS ANA Pty Ltd
trading as
ANA Loss Adjusters
ABN 78 163 470 255

Level 25, 100 Mount Street
North Sydney, NSW 2060

Phone (02) 8459 7056

manager@ana.net.au
www.ana.net.au

Updated 21 March 2023

Contents

1 Purpose and Principles

1.1 Purpose

We work in an increasingly complex legislative, technological, business and risk environment.

Information management has become critical to business success. Information is valuable and subject to exposure and contamination risks.

Managing and protecting information is especially important to ANA as we manage confidential information on behalf of our clients and their clients.

The need to protect information can conflict with business needs to use that information, creating pressure to relax and compromise security.

The role of this Consolidated Information Technology Security policy is to protect information, to maintain that protection and enhance it in response to new and expanding threats, while supporting legitimate operational access.

1.2 Principles

The principles underpinning this policy are:

Data ownership

Data given to us by and on behalf of our clients belongs to those clients: we are custodians of it. We must preserve and protect it, keep track of its use, movements and storage and return it when required, ensuring no unauthorised copies are retained.

Data value

A standard approach to cyber risk management is to rank data according to its value, reflecting:

- The consequences of data loss and/or exposure
- The cost of rebuilding the data.

In the case of client personal (data supplied to ANA by the insured) ANA does not have the information nor the right to make such value judgements.

Accordingly, all Client data is rated at highest value and receives our highest level of protection.

Storage points

The more places there are storing copies of a particular data set, the greater the vulnerability. ANA is committed to best practice in terms of ongoing development of tools and solutions to give our clients optimum protection around minimal storage points for their information whilst in our care.

Data security

ANA will maintain industry best practice security for stored data, including data encryption, pro-active monitoring of traffic for suspect content according to regularly updated profiles of known sources and identification if suspect data forms and situations and offsite backup.

Right-to-know, need-to-know access

ANA contracts with clients specify who will have access to their data: this sets a right to know.

Those with a right to know are still only granted access on a need-to-know basis e.g., only Adjusters actively working on an account will have access to that account.

Further, access will be restricted to sections of the information relevant to work being done at the time.

Finally, access shall be time-specific and not continue indefinitely: when the right-to-know or need-to-know are revoked or expired, access will be closed.

Access control including confirmation of identity and 2FA

Data access will only be given to people whose identity and authority have been confirmed.

Two factor authentication will apply to all log-ins.

Logging

All access to, use of and transfer of data from our CMS will be logged and searchable to enable tracing of any incidents.

Only the ANA Security, Privacy and Data Protection Officer (SPDPO) shall have access to the logs. The SPDPO may delegate time-restricted access as required to deal with issues. Logs are set to be not alterable.

1.3 Carriage of this policy

The ANA Security, Privacy and Data Protection Officer (SPDPO) is responsible for the carriage of this policy, including its documentation, implementation and ongoing development.

2 Data structure and management

2.1 Management

Data management is the responsibility of the ANA Security, Privacy and Data Protection Officer (SPDPO), who reports direct to the CEO.

Responsibility includes:

- Ensuring all staff are trained in and adhere to the policy.
- Developing and updating the policy to meet new demands and take advantage of new technologies and practices.
- Implementing changes including updated training.
- Managing approved access, ensuring secure logins.
- Annually in June reviewing the state of IT security across ANA’s operations, including:
    - information assets and technologies,
    - PEN test results during the year,
    - compliance with security policies,
    - technical compliance of IT systems,
    - a revised assessment of exposure to information security and privacy threats,
    - and a written report to the CEO with any recommendations including enhanced policy and technology options.
- Also included in the annual review will be specific audits of the security of each Insurer’s data, with individual written reports to each Insurer.
- Conducting such other reviews as beneficial during the year.
- Contributing to IT planning including hardware and technologies and the development of an IT roadmap.
- Documentation of ANA decisions affecting IT policy and practice into a readily accessible document and dissemination of that information as appropriate.
- Change management for changes in IT structure and practice.
- Maintaining compliance with all legislation including privacy and breach reporting.
- Maintaining compliance with all contractual security obligations.
- Documenting IT procedures etc in a manual.
- Developing tools to detect policy non-compliance by staff, suppliers and clients.
- Contributing to the maintenance and development of the ANA Business Emergency/Disaster Continuity Plan and supporting structure, as it relates to IT Security.
- Responding to all security incidents, including participating in the ANA Emergency Response Group (ERG) in response to major incidents involving IT risk or breach.

2.2 Data model

The ANA data model defines the process for the handling of data.

Data storage

The primary storage for all client data is the ANA Claims Management System (CMS), which is highly secure and controllable environment with the WebVault Perth facility, providing a very high level of security.

No paper copies are held.

When data and client contact details are received by ANA via inbound email it will initially be present (stored) in ANA email systems.

Documents (attachments) received this way will be uploaded to the client area in the CMS and then deleted from the email system, thus maintaining the CMS as the primary source of data.

In summary, the ANA data storage model aims to store all client data in the CMS, where it is most secure.

Data transfer

Information and documents received and created by ANA relating to a client are uploaded from the ANA email system to the CMS.

Data retention and disposal

Customer-specific data can be deleted from all ANA systems on the request of our client, otherwise it is held for 10 years.

Every year in June and in December the SPDPO will review the CMS for customer data more than 10 years old and delete it.

Data deleted from the ANA CMS is deleted from the server.

Deleting customer specific data

Customer-specific data can be deleted from all ANA systems on the request of our client.

Data types

Data entered directly into the ANA CMS is entered as text.

Documents can be uploaded for storage in any format but will require appropriate software to read them.

2.3 Data security at rest

Customer data in the CMS is secured at rest:

- at the application logic level, and
- via WebVault data centre security, which is multi-faceted, industry-leading and constantly evolving.

2.4 Access policy

The ANA Access Management Policy is based on the principles of right-to-know and need-to-know.

Identity

Users must be able to demonstrate on seeking access that they are who they say they are.

Acceptable for this is a combination of:

- Company-based email address.
- Password
- 2FA via a validated mobile device.

Right to know

For ANA clients, the user's right of access must be validated by a written authority from the client.

ANA contracts with clients may also specify who will have access to their data and this sets a right to know.

For ANA staff, access rights must be approved by the manager of that ANA office or by the CEO.

Only ANA staff actively working on a claim, plus accounting and management functions, will have access to personal details of people connected to that claims.

Need to know

A user's log-in credentials may give them access to a wide range of data, but they should only use that access to view or act on data where they have a legitimate need to do so, in order to fulfill their duties.

In the first instance this is a professional obligation that requires the user to exercise judgement and restraint. In the event of an issue however user file actions can be tracked via CMS logs.

Further, access will be restricted to sections of the information relevant to work being done at the time.

Time specific access, termination and review

Access permissions may be granted as time specific, to be expire after a set period.

Access permissions can be revoked by the Client in the case of client users and by ANA managers.

The SPDPO shall review the full list of people with access at least quarterly and remove redundant permissions.

Access control including confirmation of identity, 2FA, passwords

Data access is only be given to people whose identity and authority have been confirmed.

Two factor authentication will apply to all log-ins.

User names must be email addresses based on approved company URLs.

Passwords must be complex according to rules set and adjusted by the SPDPO from time to time and they must be unique within the CMS. Passwords may not be re-used.

New accounts

New account requests must be reviewed by the SPDPO in accordance with this policy, paying particular regard to authorisation, confirmation of identity, minimum permissions based on need-to-know and agreement to this policy.

The SPDPO will then make a recommendation to the CEO.

Applications approved by the CEO will then be actioned by t

Passwords will be confirmed separately from notification of approval and user name, user via SMS. New users are required to change their password on first login.

Brute force lock-out and tracking

Only three consecutive attempts at log-in are permitted. A fourth failed attempt locks the user out for 30 minutes, guarding against brute force password attempts.

All log-in attempts are logged with IP address and data kept for at least three months.

The SPDPO at least quarterly reviews log-in logs to identify repeated failed log-ins, identify the source and black list the IP address if it is not linked to an authorised party.

Logging

All access to, use of and transfer of data from our CMS will be logged and searchable to enable tracing of any incidents.

Administration of access rights

Access rights including log in credentials and verified 2FA devices are administered by the SPDPO.

2.5 Developer access

Developer access is generally restricted to the development environment, which is sandboxed from the production environment, and further restricted to software code or dummy test data, with no access to customer data.

It is possible that broader access could be required, for example to track malware and other hostile code and to repair data errors. Is such a case the SPDPO shall:

- Notify the CEO immediately
- Make a reserve back up copy of the data.
- Personally or via ANA's Head of Software Development supervise the work at all times, with either physical oversight of the coder or on-line supervision of activities.
- Developer access is always time-limited in line with a project and is not continuous.

2.6 Standards development

The ANA Security, Privacy and Data Protection Officer (SPDPO) is responsible for:

- Documentation of ANA's own IT Security Standards.

- Ensuring training for staff, leading to understanding of and adherence to the ANA IT Security Standards.
- Ongoing development of the ANA IT Security Standards to ensure their effectiveness and delivery of best practice outcomes.
- Monitoring development of recognised certified standards schemes such as Information Security Standard (ISO/IEC 27001 and 27002, Cyber Security Standards, National Institute of Standards and Technology NIST and others, especially noting any developments it would be advantageous for ANA to introduce and, in consultation with the CEO, adapting them into the ANA IT Security Standards.

- The SPDPO is responsible for monitoring, assessing and testing overall security effectiveness, including reporting to the CEO, and may elect to use external audit services where this is cost effective.

2.7 Enforcement

Non-compliance with the ANA Consolidated IT Security Policy is regarded by ANA as a serious failure of employment obligation.

Supervising managers are charged with detecting non-compliance and reporting it to the ANA Security, Privacy and Data Protection Officer (SPDPO).

The relevant manager and the SPDPO will then review the non-compliance and decide a course of action, which will include:

- Discussing the non-compliance with the staff member, to ensure they understand:
  - What was required of them
  - Why the requirements are important and the possible implication of their behaviour to the business.
  - What is required of them going forward.
- The possible disciplinary consequences of their actions, including formal letter of warning or in cases of serious breach of trust and duty or refusal of instruction, summary dismissal.
- What further training the employee should receive.
- If indicated, a referral for counselling.
- Creation of further workplace supports to make compliance easier.
- Ongoing supervision arrangements to ensure compliance (type of supervision and duration).
- Whether the problem represents a more widely spread attitudinal or informational problem, and steps to alleviate that such as additional training and reminders of policy.

The SPDPO and the relevant manager will decide and implement an appropriate disciplinary action, which may range from:

- Formal discussion and advice.

- A written advice and instruction of compliance.
- A formal letter of warning.
- Summary dismissal.

2.8 Privileged Access Management (PAM)

ANA's Privileged Access Management (PAM) system is reflected throughout the ANA Consolidated IT Security Policy.

ANA's PAM includes multiple cybersecurity strategies and technologies for monitoring and controlling privileged access, (user accounts). Central is the principle of least permissions, that users have only the access they are authorised for and cannot extend their use of the system beyond that.

See also Section 6 Protecting data and access.

3 Data and access devices

3.1 IT assets management

ANA's hardware structure is straightforward and limited, creating an environment which makes it easier to enforce a high level of security.

The ANA Security, Privacy and Data Protection Officer (SPDPO) maintains a register of all company and approved BYOD hardware assets, including:

- Physical location (or base for mobile devices)
- Person responsible and authorised to use
- Permitted uses (specific data etc.)
- Manufacture date, expected lifecycle
- Any associated licences including renewal dates

The ANA SPDPO maintains a similar register of all software installed on company and approved BYOD hardware assets, including:

- Installed software systems
- Any associated licences including renewal dates
- Remote monitoring and wiping protocols

The SPDPO reviews these asset registers on an ongoing basis, including full reviews once a year in December/January.

3.2 Hardware

3.2.1 CMS hosting

The CMS is hosted by DataVault in Perth, which is an accepted industry best practice for private and government data storage and service that gives a very high level of protection.

- Tier 1 data centres apply industry-leading and continually evolving data access protections.
- Second geographically isolated Tier 1 data centre for backup/data recovery
- VMware vSphere Cloud operating platform providing Virtualised Servers (Platform as a Service PaaS).
- Fine-grain identity and access controls including 2FA (two factor authentication) combined with continuous monitoring for near real-time security information.

Physical access is highly restricted. Employees who need physical access must first apply and provide a valid business justification. Requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access, and are time-bound. Requests are reviewed and approved by authorised personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Third party access required similar procedures plus escort by authorised staff at all times.

3.2.2 Office tech

ANA offices use standard Windows-based desktop computers and laptops, plus printers (very few client documents are printed). Brands are not restricted as brand is judged to have little impact on security.

All adjusters use smart phones with cameras. Brands are not restricted as brand is judged to have little impact on security. No client data is stored on phones, except photographs typically taken as part of claims and deleted when claims are closed.

3.2.3 Laptop computers

ANA-controlled laptops, which may be used for field work where their IP address will change with local networks, are by policy set only to view and not download data.

However, in situations of poor internet access individual adjusters in the field may on application to the ANA Security, Privacy and Data Protection Office be granted temporary download access. Downloads a made to a specific folder. On return to a stable internet area changed data is uploaded to the CMS, the folder contents deleted and download permission revoked.

3.2.4 Phones and pads

By policy, ANA users access the CMS via phone or pad only to view and not download data.

Mobile device access does allow working on and adding to data stored in the CMS.

Similarly, ANA-controlled phones and pads are by policy set to IMAP, so email viewed remains open the server and is not downloaded to the device.

3.3 Software

ANA's proprietary Claims Management System (CMS) software is the primary tool used for client work. It is a highly-secure cloud based (SaaS) with no installation on local devices.

ANA staff use global standard software for documents and communication, including Microsoft Office (Word, Outlook, Excel and PowerPoint) and Acrobat (for PDFs).

Created documents that are specific to a client are uploaded to the CMS and deleted from local devices. Documents may also be communicated between ANA and clients via the CMS, though practicality may demand in some situations (e.g., communicating with a claimant) or a client require that they are shared via email.

3.4 Software and access permissions record

The SPDPO maintains an up-to-date record of software used by ANA, including:

- Licensing
- Where it is installed
- Who has access, what they have access to.

3.5 Decommissioning

Company owned data storage devices when decommissioned are wiped using a write-to-zeros dual pass protocol and then physically destroyed either locally or via a recognised data destruction service.

This applies to hard drives (internal and external), removable drives like USB sticks and re-writable CDs/DVDs. Write-once CD/DVs are physically destroyed.

Approved BYOD devices including phones and laptops are reset to factory prior to disposal or destruction, in accordance with the BYOD policy agreed by all BYOD uses.

3.6 Removable storage devices

ANA staff are not permitted to store client data on removable storage devices (such as thumb drives).

3.7 Client access hardware

Authorised ANA clients may use desktop computers to access CMS data relevant to them, for example tracking the progress of claims.

The CMS is cloud based, so standard working practice is to view data in the Cloud and not copy it to the local device. As needed documents may be downloaded.

The IP address of desktop computer must be notified to ANA as part for the registration for access. White listing approved desktop computer IP addresses can speed user access and assists in detecting fraudulent access attempts.

Client access is specific to individuals and requires initial identity validation and 2FA login.

Clients requiring mobile access are asked to discuss this ANA State Manager or the ANA SPDPO.

3.8 IT Acceptable Use Policy

This section applies to all use of ANA provided IT tools, software and devices.

Laptops, phones and pads provided by ANA may be used for personal purposes including essential communication with family and friends during work hours and for general purposes outside work hours, subject to the following acceptable use conditions.

- Call volumes and data use shall be within normal usage and shall not impose additional costs on ANA.
- Personal use must not impede or restrict ANA-related use.
- You must not restrict the operation of ANA related software and tools, including remote-access monitoring.

In addition, you must not use the devices or services in any way that:

- Violates Australian law.
- Compromises or could compromise ANA security, especially of client information.
- Reveals ANA information or the private information of others to third parties without authorization.

- Attempts to violate the security of other online sites, eg denial of service attack.
- Violates the copyright and intellectual property rights of the owners of information or images that might be viewable online.
- Bullies or harasses any ANA or ANA client employee or any other person, including trolling.
- Accesses or disseminates information from or about sites or pages dealing in adult/explicit material, gambling, premium (pay for access) phone numbers, hate speech, exhortation to illegal activities or any illegal activity.
- Shares photos without the explicit consent of everyone depicted.
- Exposes ANA or its clients to risk or reputational damage.

This section applies additionally to all user-owned devices

In addition to the provisions above applying to ANA owned devices, all bring-your own devices must be approved for work-related use by the ANA Security, Privacy and Data Protection Officer (SPDPO) and must comply with the provisions of the ANA's Consolidated IT Security Policy relating to BYODs (Section 4).

4 Mobile Device Policy including BYOD

Use of mobile devices is essential to efficient modern loss adjusting practices.

Staff members bringing their own mobile devices is a fact of modern business life, especially in situations where the worker is mobile.

The ANA Mobile Device and BYOD Policy ensures that data integrity and security is maintained, while allowing the benefits of mobile devices, including BYODs.

All ANA staff who use mobile devices as part of their work, whether company owned or BYOD, must agree to this policy before using their devices for work and must thereafter comply with this policy.

4.1 Approval and Registration

All mobile devices used by ANA staff as part for their work must be approved by the ANA Security, Privacy and Data Protection Officer (SPDPO).

The SPDPO may refuse devices known to have security flaws or high risks and older devices that are not supported by the manufacturer with ongoing security updates.

Approval will be withdrawn when a device passes out of support.

Grey market devices may also be refused (e.g., legitimately manufactured devices purchased via other regional markets and thus excluded from local support).

4.2 Registration

All mobile devices used by ANA staff as part for their work must be registered with the ANA Security, Privacy and Data Protection Officer (SPDPO).

Registration details will include:

- Brand and model
- Serial number
- Manufacture or purchase date
- Normal home base

4.3 Data ownership and care

Work related data of all types that is temporarily stored or installed on an employee owned or provided device remains at all times the property of ANA and its clients, and under ANA control.

Staff bringing their own devices agree that ANA may access, modify and delete that data at any time and that they will facilitate those actions.

This data ownership and access obligation continues while ever company data remains on the device, even after the cessation of employment.

In agreeing to the ANA BYOD policy staff accept a responsibility of care towards data stored on their devices, to ensure it is secure, protected and not accessed in an unauthorised manner or by unauthorised entities.

4.4 Configuration

4.4.1 Computers (mobile and desktop)

The configuration of the computer must be approved by the SPDPO.

Configurations which may be rejected include:

- Apps allowing data access from any sources of malicious cyber activity as identified by the SPDPO. .
- Torrent services (person-to-person downloading, often used to evade copyright and high-risk for malicious payloads).
- Out-of-date and no longer supported systems and software.
- Apps downloaded from 3rd party stores (a recent Symantec study reported that 99% of identified mobile malware originated in third-party app stores).

Configuration aspects that are required include:

- A virus etc. protection service approved by the SPDPO that is always on and regularly updated.
- Login password or (preferably) biometric recognition.
- Screen lock after a defined period of inactivity not more than 5 minutes.
- “Find my computer” geolocation service installed and active, with remote lock and remote wipe.

Additional requirements include:

- The software installation and configuration of all computers must be open to remote inspection by the SPDPO via remote access including continuous monitoring using Microsoft InTune software, which reports on the device setup.
- Devices should be set to auto update with security patches and new versions.

4.4.2 Mobile devices

The configuration of mobile devices must be approved by the SPDPO.

It is similar to desktops. Configurations which may be rejected include:

- Apps allowing data access (including via Apps from sources of malicious cyber activity as identified by the SPDPO.
- Torrent services (person-to-person downloading, often used to evade copyright and high-risk for malicious payloads).
- Out-of-date and no longer supported systems and apps.
- Apps downloaded from 3rd party app stores.

Configuration aspects that are required include:

- Virus etc. protection service approved by the SPDPO.
- Login password or (preferably) biometric recognition.

- Screen lock after a defined period less than 5 minutes.
- “Find my computer” geolocation service installed and active, with remote lock and remote wipe.

Additional requirements include:

- The software installation and configuration of all mobile devices must be open to remote inspection by the SPDPO via remote access including continuous monitoring using Microsoft InTune software, which reports on the device setup.
- Devices should be set to auto update software.

4.5 Remote monitoring

All computers and devices approved for work use by ANA staff must have a Microsoft InTune client installed. This software automatically reports to ANA the configuration of the device including all software installed and its version.

This enables ANA to determine that the device is secure with all security patches installed, has approved firewall and virus protection active, no known high-risk software installed and has screen lock active.

4.5.1 Remote monitoring for client computers

Remote monitoring via Microsoft InTune is a key component in ANA’s capacity to ensure client data security.

The risk associated with access by a client (insurer) is no less than the risk associated with access by ANA staff, so clients (insurers) are requested to either:

- permit ANA monitoring of their nominated access computers, or
- sign an undertaking that such computers are monitored to ensure up-to-date software and security patches, the absence of high risk software and secure control over access.

The primary beneficiary of these measures is our client, giving them confidence that the data of their clients is secure. A weakness in security at any access point, whether within ANA or the client (insurer) puts that data at risk.

4.6 Device locking

All devices must have device locking that locks the screen after a period of not more than 5 minutes of inactivity and requires a password or (preferably) biometric data to log back in.

4.7 Device tracking and wiping

All mobile devices (phones, pads and computers) must have remote tracking enabled, with the capacity to remotely lock and if required wipe the computer.

Users agree to report device loss to the SPDPO immediately and to accept the ruling of the SPDPO as to when wiping should be instigated.

4.8 Device decommissioning, sale or loss

All ANA-owned devices are decommissioned according to the Decommissioning Policy included in this consolidated policy.

For BYOD device decommissioning ANA staff may give their device to the SPDPO for decommissioning or they may undertake their own decommissioning according to the SPDPO’s instructions.

For BYOD device sale or transfer, ANA users agree to wipe data according to the SPDPO’s instructions and subject to remote inspection prior to transfer of the device. This will include multiple write-to-zero overwrites and testing via a file recovery program.

4.9 Removable storage devices

ANA staff are not permitted to store client data on removable storage devices (such as thumb drives).

4.10 Use of devices in public areas

Use of devices to view confidential data in public spaces should be avoided where possible, but sometimes will be necessary to Adjusters working in the field.

Where data has to be viewed in a public space ANA staff must practice screen visibility control, eg by sitting against walls or in isolated spaces.

5 Data transfer

ANA's data model locates customer data within the cloud-based CMS where it is well protected from attack and unauthorised access. The CMS is a secure environment.

Data however has to be transferred to and from the CMS and to and from clients (insurers) and claimants, in order to process claims. This exposure is higher risk. ANA security measures focus on reducing the risks involved in data transfer and distribution, including tracking and managing the flow of information.

5.1 Restricted use of email for data transfer

5.1.1 Risks in use of email for data

ANA recognises email transmission as a major security risk that is probably the most common cause of accidental data exposure. Risks include:

- Emails being misaddressed, exposing sensitive data to unauthorised recipients.
- Emails being read in transit.
- Emails (or the information they contain) being forwarded to unauthorised recipients.
- Creation of multiple copies of files that cannot be tracked.

5.2 Data flow to mobile devices

ANA policy is that staff do not store client data (including emails) on mobile devices such as phones and pads.

These devices can view emails (and their attachments) via IMAP and view other files and notes via the CMS, including editing those files, but this access happens in the cloud. No documents are copied to the local device.

5.3 Tracking document flow

Documents uploaded to and downloaded from the CMS are logged and can be tracked to individual users.

Once an unprotected document is downloaded it can be copied and further distributed by the user and this is currently beyond normal tracking abilities.

For high value documents clients may request the document be password protected. This system is not suitable for general use:

- PDF and Word docs have inbuilt password capabilities, but – at least for PDFs – the protection is not strong. A user with the password may then make unprotected copies.
- Managing an individual document password system across multiple users is complex, time consuming and error prone. In most busy work environments the system will tend to break down as users try to circumvent it to save time.

Future systems may include embedded document unique identifiers, enabling tracing of unapproved copies to their original source.

5.4 Exceptions

To operate effectively in a busy and changing real world, given current technologies, some exceptions have to be allowed.

- Adjusters may store client data temporarily on computers while working on a claim, particularly when working in areas with poor or disrupted internet, but are required to erase such data at the earliest possible moment and always when a case is closed.
- Files may be received by ANA, including from clients (insurers) and claimants that must be downloaded to a computer and then uploaded to the CMS before being erased from the computer.
- Files created by ANA staff that are locally stored while being worked on, then uploaded to the CMS and deleted locally.
- Exigent circumstances where unusual or emergency conditions demand alternative action. Such actions are to be reported to the SPDPO as soon as practical.

A goal of ANA's ongoing security policy development is to use advancing technology. Systems and training to reduce and eventually eliminate exceptions.

6 Protecting data and access

6.1 Structural security

ANA's centralised customer data structure makes it is easier to protect customer data from attack and unauthorised access. The CMS is a secure environment.

DataVault Perth server facility is a best practice standard for Australian business and government, with very high levels of physical and virtual security maintained by DataVault.

Encryption Key Management is via the DataVault KMS system.

6.2 Access security

User access is based on:

- Validated identity.
- Strong passwords.
- Two factor authentication.
- Right to know, need to know.
- Time limited access that automatically expires if not renewed.
- Logging of all access.

6.3 Data security

- Single copy restriction on customer data documents.
- Customer data documents distributed via the CMS not email or removable storage devices.
- Logging of all customer file uploads and downloaded.

6.4 Systems hardening

ANA's Consolidated IT Security Policy is subject to continued development, including progressive systems hardening.

6.4.1 CMS hardening

- The CMS contains only current, operational software. No users can upload software to the CMS.
- Access to the CMS is constantly monitored and logged, with suspicious activity flagged for immediate action.

6.4.2 User computer and device hardening

- Centralised customer data storage and restricted customer document movement means that the risks to customer data of a user device compromise are contained.

- Computers and mobile devices with access to the CMS are required to maintain approved local firewall and virus protection.
- The state of computers and mobile devices with access to the CMS is continually monitored via Microsoft InTune, which reports on security patch updates, installed software including firewall and virus protection and suspicious activity.
- Microsoft InTune monitoring is a continuous, automated process.
- Microsoft InTune reports are used to detect and suspend device access until unauthorised items have been removed and an approved deep virus scan has reported no malware is detected.

6.4.3 Users and user reviews

- User access is reviewed every six months and all listed users checked for validity and currency. Expired users are removed. Unknown users are investigated individually by the SPDPO to determine their validity and that they do not indicate suspicious activity.
- User password change can be forced as situations demand.

6.4.4 Patches and security upgrades

All critical hotfixes are applied within one month of release and all security maintenance software is applied within three months of release.

6.5 Customer data encryption

Customer data is secure within the CMS. All data in the CMS is protected at the application logic level and encrypted in transit and at rest.

6.6 Review and ongoing development

- Ongoing development of ANA’s Consolidated IT Security Policy includes further hardening of protections on computers and mobile devices. Password control and remote device identification are continuing priorities.
- IT security policies are constantly reviewed, with a formal review and report to the CEO by the ANA Security, Privacy and Data Protection Officer (SPDPO) every January. The report includes a review of leading and emerging industry standards relating to IT security and systems hardening.

6.7 Contractor and Supplier access (including Developers)

Contractor, supplier and external developer access to the CMS is controlled by the ANA Security, Privacy and Data Protection Officer (SPDPO).

The SPDPO assesses applications based on need to know, data required or exposed, time period access is needed for, options for working only in the development site and activity monitoring options.

Contractor and supplier access is subject to live monitoring and focused on software not client data, with access to the development site not the live site.

Developer access is almost always to the development site only.

Access to software via the development site poses a low risk to client data privacy and integrity and does not include live data access. All actions are logged. Changes can be tested before applying to the live site.

6.8 Physical security

The CMS is hosted by DataVault, with a high level of physical security including:

- Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.
- Physical access is controlled at building ingress points by professional security staff utilising surveillance, detection systems, and other electronic means. Authorised staff utilise multi-factor authentication mechanisms to access data centres. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.
- Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit.
- Alternative power source, fire detections/suppression systems and temperature and humidity controls are in place.
- Second geographically isolated Tier 1 data centre for backup/data recovery

6.8.1 Office physical security

As client data is stored in the cloud-based CMS, paper documents relating to clients are minimal and access to the CMS requires 2FA even from office computers, the physical security of our offices is not an issue for client data security.

Standard physical office security is maintained, having regard to the assessed risk in each case (low in access-controlled CBD towers, higher in street-level suburban settings).

6.9 Monitoring and Backups

- Customer data in the CMS is backed up daily.
- Backups are secured and regularly tested to ensure effective data recovery.
- The CMS is monitored for availability, performance and capacity.

6.10 PEN testing

The ANA Security, Privacy and Data Protection Officer (SPDPO) performs regular vulnerability scans.

Penetration testing of the CMS is performed annually by external contractors.

The SPDPO is responsible for:

- Reporting any deficiencies revealed by PEN testing, vulnerability scanning or other means to the CEO
- Taking any urgently required immediate action
- Developing an action plan to respond to deficiencies
- Securing CEO approval
- Implementing the plan.

Time lines for remediation will reflect the complexity and seriousness of the issue, but include:

1 hour:	Take any immediately required action to control and secure the situation, including if required a service shutdown
1 hour:	Report deficiency and actions to CEO
1.5 hours:	Notice to users of any service restriction or data breach risk
24 hours:	Submit at least an outline of possible actions to the CEO
48 hours:	Submit a detailed action plan to the CEO
72 hours:	Commence remediation action plan
5 days:	Risk dealt with and full, secure service access restored.

6.11 Data requests by foreign entities

ANA policy is:

- "Follow the law"
- Immediately advise the owner of the data that a request has been made, unless this is prohibited by law.
- If ANA is not under a legal obligation to honour the request then we will only do so with the consent of the owner of the data (the Insurer).
- If ANA is legal under a legal obligation to provide the information, we will do so and advise the Insurer accordingly, unless prohibited by law.

In practice most situations will be different, depending on the nature of the agency making the request and treaty arrangements between the requesting government and Australia and use of Letters Rogatory.

When a request is received we will seek appropriate advice on our legal obligations in that situation.

We will share that advice with the Insurer unless prohibited by law.

7 Human resources

Security surveys regularly report staff as contributing to security breaches, most often through lax procedures and carelessness, often enabled by a culture that downplays security risks.

ANA management and policy reinforces a culture that recognises security as a top-level issue, adheres to a detailed security policy and practice and responds to risks and potential compromises.

7.1 Employee selection

The ANA Employment Policy includes assessment of candidates' understanding of data security and client privacy policies, laws and practice.

The selection methodology includes screening via interviewing professional referees, including questions about ethics of and practical attitude towards security and privacy.

New employees are required to agree to and sign a range of documents including an NDA/confidentiality agreement, code of ethics and practice and a BYOD and Working From Home Policy

7.2 Employee training

All staff receive formal induction training covering:

- Company policies, practice and culture.
- Use of the CMS including out-of-office.
- Various legislated obligations (including the Privacy Act and mandatory privacy breach reporting).
- Vulnerable customer training (ANA-developed on-line module).
- Security training (AMA-developed on-line module).
- Consequences of non-compliance.

Further training includes:

- Annual (refreshers on changes to privacy, security and vulnerable customer policies)
- Ongoing (on the job and under supervision)
- Professional Development (formal courses, professional seminars etc) training is required.

7.3 Employee agreement

All staff are trained in this policy (the ANA Consolidated IT Security Policy) at induction, with update training as needed.

All staff are required to confirm their understanding of and agreement to abide by thus policy, by signature.

7.4 Employee and contractor termination

ANA’s standard practice for employee and contractor termination includes:

- Immediate departure for dismissals (payment in lieu of notice).
- Supervised office clearing and departure.
- Return of keys and access cards etc before leaving.
- Return of company owned devices (phones, laptops) with access (working password or factory reset).
- Supervised clearing and return of company owned vehicles.
- Cancelling of all CMS and other access passwords (building, computer, email, phone, laptop) etc before the dismissed employee leaves the building.
- Pre-set email to all staff announcing the departure, with advice on security measures and ongoing work-based contact.

The goal of this policy and procedure is that dismissed employees have no access to ANA services or facilities from the moment their dismissal process is completed.

Note also that this policy includes prior management-level consideration for the provision of security during the dismissal and counselling to the dismissed employee.

7.5 Contractors and Third Parties

- Third party access to ANA computers and devices requires SPDPO approval.
- Contractors and other third parties requiring access to computers are required to complete the ANA Security Training module and to sign their agreement with the ANA Consolidated IT Security Policy.
- Contractors who will work on coding for the CMS are required to have undertaken secure coding methodology training.
- Login details are issued on a right-to-know, need-to-know bases and are assigned to individuals for personal use, including identity verification and person 2FA.
- Login details give access only to necessary areas and automatically expire after a set time period (minimum permission).
- The Third Party/Contractor agrees not to access, copy, transmit or otherwise access client data.
- All data and code the Third Party/Contractor accesses remains the property of ANA and its clients.
- All ANA data and code will be deleted from all devices controlled or used by the Third Party/Subcontractor on completion of the service.
- The Third Party/Contractor agrees to their actions being tracked and logged while working on ANA systems or premises.
- The ANA Security, Privacy and Data Protection Officer (SPDPO) will conduct random checks of the logs of contractor activity.

- All contractors and third parties will be required to sign an agreement to the above conditions, which will include a service level agreement clause or clauses as appropriate to the work, before being given access to ANA systems.

8 Passwords and password management

8.1 Strong passwords

Passwords standards are set from time to time by the SPDPO, including password strength, pass-word re-use and password changes.

Generally passwords must be:

- Strong (at least 8 characters, containing at least one lower case letter, one upper case letter, one number and one symbol, unless device restricted, eg phones).
- Not obvious no dates, names or common words)
- Unique (not used in more than one situation)
- Not written down anywhere

8.2 Single sign on services

BYOD users may use their own single sign on service (password manager), if it is approved by the SPDPO.

The ANA security road map includes a company-wide single sign on service enabling:

- Centralised control
- Time specific temporary passwords
- Automated password changing
- Automated password generating
- Weak and duplicated password reporting

9 Incidents

9.1 Incident reporting and register

All staff are required to report all security issues, breaches, attempted compromises, policy failures and suspicions to the ANA Security, Privacy and Data Protection Officer (SPDPO).

In doing so, staff may request and shall not unreasonably be refused anonymity and whistle-blower protections.

All reports shall be documented and assigned an incident number, in an IT Security Incident Register maintained by the SPDPO.

The SPDPO shall promptly and thoroughly investigate all such reports, having regard to whistle-blower protections and anonymity. Actions will be documented by the SPDPO in the IT Security Incident Register, through to closure of the incident.

9.2 Incident response

- Events where no client data has been exposed may be dealt with by the SPDPO alone, or the SPDPO may elect to involve others as necessary to secure a better outcome.
- More serious issues will be dealt with by the SPDPO working with the appropriate supervising manager as a response team to investigate and resolve the situation. The SPDPO may elect to notify the CEO as appropriate.
- Incidents involving exposure of client or other sensitive data shall be notified immediately to the CEO who may elect to join or send a delegate to the response team.
    - The response team shall track and respond immediately to any trigger of mandatory reporting obligations under the Privacy Act and Notifiable Data Breaches (NDB) scheme.
    - The supplier of the information (eg, the Insurer) will be notified within 24 hours and then any individuals who are the subject of the disclosure within 36 hours. The NDB scheme requires we notify affected individuals but we can liaise with the Insurer about how this is done in the 12 hour gap.
    - Insurers may elect to send a delegate to work with the response team.
    - The Insurer will receive a daily written report of progress and developments.
- Incidents which pose a threat to the ongoing continuity or sustainability of the business will trigger the ANA Business Emergency/Disaster Continuity Plan, as set out further on

9.2.1 Ongoing risk mediation

The SPDPO shall assess the risk of the incident expanding (e.g., continued hostile penetration of data) and shall establish containment as needed, such as:

- Reduced CMS or other software functionality or access.
- Temporary closure or demounting of the CMS.

- Application of additional protections, firewalls etc.

9.3 Incident closure

Incidents shall be closed on the decision of the SPDPO, with the entry into the IT Security Incident Register of a reason for closure. Reasons may include:

- No risk, no action.
- Risk but no exposure, remedial action taken (e.g., training, policy change, password resets, changes to security settings).
- Minor event with no customer or company data compromise, dealt with by staff counselling/training and/or changes to procedures including adjustments to security settings (e.g., firewalls, forced password resets etc.).
- Significant event dealt with by tailored actions (detail).
- Major event (client data exposed/compromised) dealt with by tailored actions (detail). Note whether client is now satisfied.
- Disaster response triggered.

Incident closure notes should also include:

- Successful completion of a system scan and other tests as appropriate (e.g., a PEN test after cleaning of a successful penetration attack) to confirm system integrity.
- An ongoing risk assessment.
- Recommendations for further action.

The SPDPO shall in their annual report document all security breach reports received, breaking them down by type, severity, consequences and outcome including remediation and ongoing changes, including suggesting actions to learn from the experiences.

9.4 Incident remediation timelines

Speed of resolution is critical with data breach incidents, especially when customer data has been compromised. Starting from the SPDPO's receipt of a report or other indication of an incident (e.g., automated firewall reporting) our target timelines are:

1 hour SPDPO assigns an incident number in the IT Security Incident Register and commences initial investigation.

3 hours Initial assessment of incident severity (focusing on risk of client data exposure) and drawing in of other people as needed.

4 hours Shut-down of CMS or other services or restriction of access as necessary.

24 hours Notification to clients and NDB scheme of any customer verified data breaches.

36 hours If the CMS is shut down, mount back-up copy to a new server container to restore limited functionality (all passwords reset).

48 hours Minor incidents resolved.

48 hours Engage with individuals whose data has been breached to support them.

3 days Full restoration of service via restored backup.

4 days Identification of vulnerability/breach of policy that enabled the incident, commencement of remedial action.

5 days Resolution with affected individuals.

7 days Incident closed.

9 days Written report from SPDPO to CEO.

10 days CEO supplies report to client (insurer).

15 days CEO and SPDPO meet with client (insurer) to resolve any outstanding matters.

10 Disaster management

Serious IT incidents are managed according to the ANA Business Emergency/Disaster Continuity Plan, which specifies management actions in extreme circumstances, including:

- Convening of a pre-defined ANA Emergency Response Group (ERG) and response structure.
- Assumption by the ERG of enhanced management authority with shortened decision making processes as necessary to the situation.
- Access to additional resources to enable to the ERG to deal with the emergency situation.
- Support to staff.
- Procedures for restoration of normal activity
- Learning from the experience to avoid similar events in the future.

11 Systems and policy development

11.1 CMS development

ANA’s CMS is subject to continued development.

- Systems planning including development goals, architecture and design, testing, release and maintenance are managed by the ANA Security, Privacy and Data Protection Officer (SPDPO), working in consultation with the CEO and the developer.
- Development is via a secure systems development processes (SDLC) including:
  - There is a segregated development environment that does not affect the live environment and does not give access to live data.
  - Pre-release testing is done in the development environment. It includes code review, vulnerability scanning and sign-off prior to going live
  - ANA delivers its CMS development in-house, without using third parties or contractors.

11.2 Policy development

ANA’s Consolidated IT Security Policy are subject to continued development.

The SPDPO makes recommendations to the CEO on an ongoing basis and in the annual report and implements these as agreed.

This policy is updated accordingly. Changes are promoted to staff.

ANA’s IT security training model is also updated accordingly and staff required to retake the training or an update training.

12 Training

The ANA Security, Privacy and Data Protection Officer is responsible for:

- Ongoing development of the ANA IT Security Training Module.
- Ensuring all new ANA staff promptly complete the ANA IT Security Training and Assessment, to ensure their understanding
- Ensuring all new ANA staff promptly complete the ANA IT Security Training and Assessment, to ensure their understanding
- Ensuring all new ANA contractors and suppliers complete the ANA IT Security Training and Assessment (Suppliers), before they provide services.
- On request, arranging training for ANA clients to enable them to understand their interface with the ANA IT Security Policy.
- Advising all staff, suppliers and clients of changes to the policy during the year.
- Ensuring all staff complete IT Security training updates whenever there are significant changes.
- Encouraging staff feedback on changes as part of a change management process.
- Maintaining compliance with the policies.

12.1 Training objectives

The ANA IT Security Training Module will include:

- General information on security awareness.
- Breach risks and consequences.
- Accidental exposure and facilitation.
- Risk of internal breach.
- Dynamic, pro-active approach.
- Reporting suspicious activity.
- Password and 2FA security.
- Malware/hacker controls.
- Incident response.
- ANA Consolidated IT Security Policy.
- Clear desk policy
- Inclusion of suppliers and clients in security net.

Versions of the training will specifically address suppliers and clients.

12.2 ANA staff

ANA staff on commencement must successfully complete the ANA IT Security Training and Assessment and also the annual update in December/January.

ANA staff must in practice adhere to the IT Security Policy. Assessment of adherence is a standard part of ANA performance review procedures.

All staff must complete privacy training annually by June and report course completion to the SPDPO, who follows up any staff not reporting compliance by 30th June.

We use the Privacy Training provided by Office of the Australian Information Commissioner at https://education.oaic.gov.au/elearning/privacy-in-practice/welcome.html

12.3 Suppliers

Suppliers are bound to the ANA Consolidated IT Security Policy, specifically including:

- Data ownership, copying and tracking; surrender/destruction of data.
- Right-to-know and need-to-know access.
- Password and 2FA security, including not sharing and not leaving unattended screens with open docs.
- Acceptance of activity logging.

12.4 Clients

Client staff accessing the ANA CMS are bound by the sections of the ANA Consolidated IT Security Policy that relate to them, including:

- Password and 2FA security, including not sharing and not leaving unattended screens with open docs.
- Right-to-know and need-to-know access.
- Acceptance of activity logging.
- Obligation to promptly notify ANA of staff departures or change of role affecting access rights.

13 Ongoing evaluation and development

Responsibility for ongoing review of these policies including:

- Reviews
- Audits
- Training
- Testing
- Development
- Reporting

Is governed this policy under the direction of the ANA Security, Privacy and Data Protection Officer (SPDPO), reporting to the CEO and Executive Chair.

13.1 Reviews and audits

Essential to ongoing development of this policy is that the systems it describes are evaluated, to check their implementation and effectiveness and guide any needed improvement or extension.

13.1.1 Reviews

The SPDPO is responsible for several formal and informal reviews over the year.

The SPDPO can also initiate reviews where there is an apparent need, in response to events, or as directed by the CEO or Executive Chair.

Included are:

- Review of data access applications with report and recommendation to the CEO for approval of access.
- Review of data access approvals including deletion of no longer needed or expired credentials.
- Review of attempted intrusion reports, access logs, hosting performance measures and other security matters.
- Review of passwords including regularly changes, forced resets and use of single point access tools.

The SPDPO documents all reviews but need not report them formally at the time, unless there is a need (eg, for action to be taken) or a direction from the CEO or Executive Chairman.

The SPDPO will list all reviews with dates and outcomes as part of their annual It Security Report,

13.1.2 Audits

An external security review will be conducted annually using the Essential 8 framework, and reported promptly to the CEO.

The SPDPO can also initiate additional internal audits where there is an apparent need, in response to events, or as directed by the CEO or Executive Chair.

The SPDPO manages additional external audits approved or directed by the CEO.

13.2 Training

Usually training is necessary to ensure people know, understand and follow policies.

Training directed by the SPDPO includes:

- Privacy (annual refresher).
- IT security awareness training via the ANA IT Security Training Module.
- ANA policy knowledge via the ANA IT Security Training Module.
- Password and access management .

13.3 Testing

The SPDPO will commission and report on penetration testing by a external body at least annually and more often in response to circumstances, including after any major incidence.

The SPDPO will devise a range of scenarios to be used in training simulations, with at lest one exercise per year to be conducted to response to test each of:

- Incident management and response under this policy.
- Disaster recovery under the ANA Business Disaster Continuity Plan

The results of PEN testing and simulation exercise will be reported in the SPDPO's annual report.

13.4 Policy development

This policy has evolved through several versions and must continue to develop to meet changing needs.

Any ANA employee, manager, committee or client may suggest improvements to ANA's IT Security policies.

Suggestions will be evaluated by the SPDPO resulting in recommendations to the CEO and on the CEO's decision a feedback response to the originator of the suggestion.

All significant changes to policy must be subject to a change management process to be delivered by the SPDPO and including:

- Consultation and review as needed.
- Decision documentation and dissemination.
- Documented implementation strategies, timelines and assessment.
- Provision for feedback and review during implementation.
- A completion report to the CEO with a version for staff dissemination, if dissemination of the full report is not appropriate.

13.5 Reporting

The SPDPO will in June each year prepare a written report of the state if IT Security over that financial year and present a draft of this to the CEO in July.

The report will include:

- A summary of developments, changes, improvements and events/incidents during the year passed.
- A listing of all reviews and audits carried out during the year, with details as appropriate.
- A listing of all security incidents during the year, with details as appropriate.
- A list of security related training conducted during with a review of outcomes and effectiveness.
- A succinct summary of the state of IT security at ANA.
- Recommendations for action, grouped by urgency and showing estimated cost.
- A proposed schedule and budget for the year, covering:
  - Security costs
  - Training
  - Independent (third party) tests and audits including PEN testing and auditing against the Essential 8 security framework

When the report is finalised it will be available to Clients (Insurers) on request and by agreement.