INFORMATION SECURITY MANUAL

Last Reviewed	**April 2023**
Next Review	**January 2024**
Responsible Officer	**Governance & Projects Specialist**
Applicable Legislation	**Privacy Act 1988 (Cth)**
Relevant Policies	
Related Procedures	

WAFC CORE VALUES

Our People | Our Relationships | Being our very best | Leading our Industry

PURPOSE

WAFC staff have a legal obligation to manage the Information Assets of the West Australian Football Commission Inc. in accordance with relevant Information Security & Privacy legislation and laws during the day-to-day operation of our business.

Document Integrity Control			
Filename:	WAFC Information Security Policy		
Version:	2.0		
Version	**Authorised By**	**Action**	**Effective Date**
1.0	Risk & Gov. Committee	Initial draft prepared by Squire Patton Boggs (AU)	NA
2.0	Risk & Gov. Committee	Final Copy adopted	16th June 2023

As at the date of this Policy:	
The **Information Security Committee Chair** is:	**Linda Hamersley** Executive Manager Operations & Capability
The **Information Security Officer** is:	**James Hunt** Governance & Projects Officer
The **Information Technology Manager** is:	**Gihan Dhanushka** IT Support Specialist

CONTENTS PAGE

1 DEFINITIONS & INTERPRETATION

1.1 Defined terms

In this Policy:

Terms defined throughout, as indicated in bold within parentheses, have the meaning given therein; and

Business Day means a day that is not a Saturday, Sunday, public holiday or bank holiday in Perth, Western Australia.

Human Resources means the Staff Members engaged to provide human resources services to the Organisation and manage employment.

Information Security Committee Chair means the chairperson of the Information Security Committee.

Information Security Officer means the Staff Member with delegated authority for the adoption, implementation, review, management and enforcement of this Policy within the Organisation.

Information Technology Manager means the Staff Member designated as the manager of the Organisation's Information Technology Staff.

NDB Scheme means the Notifiable Data Breach Scheme established under Part IIIC of the Privacy Act.

OAIC means the Office of the Australian Information Commissioner.

Policy means this information security policy.

Privacy Act means the *Privacy Act 1988* (Cth).

1.2 Interpretation

In this Policy, except where the context otherwise requires:

(a) a reference to "the Organisation", "we", "our" or "us" is a reference to **The Western Australian Football Commission Inc.**

(b) a reference to "you" refers to the individual reading this Policy and who is subject to the controls and obligations outlined within;

(c) the singular includes the plural and vice versa, and a gender includes other genders;

(d) another grammatical form of a defined word or expression has a corresponding meaning;

(e) a reference to a section or paragraph is to a section or paragraph of this Policy;

(f) a reference to a document or instrument includes the document or instrument as novated, altered, supplemented or replaced from time to time;

(g) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them; and

(h) the meaning of general words is not limited by specific examples introduced by *including*, *for example* or similar expressions.

2 POLICY MANAGEMENT

Objective	The purpose of this section is to provide management direction and support for information security in accordance with our business requirements and relevant laws and regulations.

2.1 Information Security Policy

The Organisation has designed, authorised and issued this Policy to address our management of personal information and data security risks by outlining the Organisation's minimum requirements and expectations in the pursuit of maintaining the confidentiality and integrity of information under our control while ensuring the availability of information in the best interest of the Organisation's operations.

The Organisation accepts that by merely adopting this Policy, in and of itself, does not ensure the actual or cultural compliance with the principles and policies outlined by this Policy within the Organisation. It is our commitment to ensure that the principles and polices outlined in this Policy become a practical and cultural reality for the Organisation in all respects.

This Policy has been adopted by the Organisation on the date appearing on the inside cover of this Policy and is effective from that date. Any subsequent amendments or variations may only be made via a resolution of the Organisation's board or by the Information Security Officer exercising delegated authority. Any amendments or variations to this Policy are recorded in the table appearing on the inside cover of this Policy and are effective from the corresponding date shown.

2.2 Review of Policy

(a) The Organisation will review the operation of this Policy against measurable and qualitative benchmarks having regard to the results of any audits undertaken pursuant to section 12 and generally accepted good practice information security standards as they develop from time to time (**Review**).

(b) The Organisation will periodically Review this Policy, desirably on an annual basis, and will Review this Policy at such other times as decided by the Information Security Officer or in the event of any significant change to the Organisation's commercial, legal or regulatory outlook or in the event of a substantially progressed technical or operational environment.

3 OVERVIEW

This Policy establishes a policy-based control framework designed to ensure ongoing information security within the Organisation. This Policy has been drafted and implemented in accordance with industry best practice standards established by the Australian and New Zealand ISO/IEC 2700 series information security standards.

3.1 Information Security

Information security within this Policy is defined as the preservation of information controlled by the Organisation with reference to three principles:

(a) **confidentiality** – ensuring that information is not made available or disclosed to unauthorised individuals, entities or processes;

(b) **integrity** – ensuring the accuracy and completeness of information and systems that process and store information; and

(c) **availability** – ensuring that information is accessible and usable on demand by authorised individuals within the Organisation.

3.2 Scope

This Policy is applicable to the personnel, facilities and systems of the Organisation and information that is collected, accessed, used, handled and transferred in connection with our business operations and applies to:

(a) the Organisation's employees and independent contractors (together, **Staff Members**); and

(b) external third-party service providers engaged in connection with the Organisation's business operations or hosting information or communications technology infrastructure and services on our behalf.

4 INFORMATION SECURITY MANAGEMENT

Objective	The purpose of this section is to establish a management framework to initiate and control the implementation and operation of information security within the Organisation.

4.1 Information security roles and responsibilities

Control	To define and allocate information security responsibilities across the Organisation.

All Organisation Staff Members and external service provider personnel are responsible for ensuring that the Organisation maintains a high standard of information security by implementing the controls and meeting the objectives outlined in this Policy.

The Organisation allocates responsibilities for information security as follows:

Personnel	Responsibilities
Information Security Committee	A committee consisting of relevant Executive Managers, the Information Security Officer and the Information Technology Manager (**Information Security Committee**) are responsible for general policy considerations regarding the Organisation's information security position, the development and adoption of this Policy and the Policy's ongoing implementation and adaptation.
Information Security Officer	The Information Security Officer is responsible for ensuring the practical adoption, implementation, review, management and enforcement of this Policy and is delegated authority to determine the compliance of procedures, activities or specific actions in accordance with this Policy.
Information Technology Staff	Staff Members employed to implement, manage and operate the Organisation's information technology systems are designated in this Policy as information technology staff (**Information Technology Staff**). In addition to the general obligations regarding information security applicable to all staff members, Information Technology Staff have a responsibility to ensure that the Organisation's information processing systems and information technology systems operate in accordance with this Policy.
Information Processing Staff	Staff Members who engage in the collection, management or processing of information are designated in this Policy as information processing staff (**Information Processing Staff**). While all Staff Members have a responsibility to comply with this Policy, the Organisation recognises that Information Processing Staff regularly engage with or deal in the Organisation's information and information processing systems and expect that Information Processing Staff are aware of and compliant with their obligations under this Policy at all times.

General Staff	Staff Members and contractors who do not engage in the collection, management or processing of information are considered to be general staff (**General Staff**). General Staff must ensure that the Organisation's information and information processing systems are protected from misuse, unauthorised access or disclosure and destruction at all times by complying with this Policy.
Third Parties	External third parties may have access to the Organisation's information or information processing systems and, to the extent that they do so, the Organisation will generally require that they comply with relevant provisions of this Policy when doing so. The specific obligations of third parties pursuant to this Policy will be prescribed in the Organisation's contractual agreements with those third parties.

4.2 Segregating duties

Control	To segregate conflicting duties and areas of responsibility in the interest of reducing opportunities for unauthorised or unintentional modification or misuse of the Organisation's information assets.

The Organisation prohibits the same person from occupying the roles of Information Security Officer and Information Technology Manager simultaneously.

To the extent this Policy provides the Information Security Officer or Information Technology Manager with powers to direct or authorise actions in relation to information security, the Information Security Officer or Information Technology Manager must record, or provide for the recording of, each individual exercise of those powers in a log (**Authority Log**). The Authority Log must be jointly accessible by the Information Security Officer, Information Technology Manager and the Information Security Committee Chair and updated by the relevant parties in real time or as soon as reasonably practicable afterwards.

The Authority Log must be reviewed by:

- the Information Security Committee Chair at each committee meeting; and
- any auditor conducting an audit of the Organisation's information security practices pursuant to section 12,

for the purposes of identifying any inconsistencies between the Authority Log and actual actions taken by the Organisation or its Staff Members which may suggest the accidental or deliberate misuse of the Organisation's information assets.

4.3 Contact with authorities and special interest groups

Control	To maintain appropriate contacts with relevant authorities, special interest groups or other specialist security forums and professional associations.

The Information Security Officer is expected to be aware of and maintain appropriate contact with relevant regulatory bodies and supervisory authorities to the extent necessary to ensure the Organisation continues to meet the objectives outlined in this Policy.

In addition, maintaining such contacts may be necessary to ensure timely responses to information security incidents or data breach incidents in accordance with the obligations outlined in sections **Error! Reference source not found.** and 10 r espectively.

4.4 Information security in project management

Control	To address information security in project management functions moving forward.

The Organisation considers that information security must be integrated into the Organisation's project management methodologies to ensure that information security risks are identified and addressed during project management. The Staff Member responsible for the development and implementation of a particular project must collaborate with the Information Security Officer and Information Technology Manager to:

- provide for information security objectives to be included in project objectives;
- undertake an information security risk assessment at an early stage of the project to identify the potential risks arising out of the management of information by the project and to prepare controls designed to limit those risks; and
- ensure that information security considerations are included as a part of each phase of the project's methodology, including implementation, review and decommissioning.

This section applies to every project commissioned by or for the Organisation, regardless of its scope or operation and includes core business processes, information technology processes, facility management and other supporting processes.

5 PERSONNEL SECURITY

Objective	The purpose of this section is to ensure: I. that Staff Members understand their responsibilities and are suitable for the roles for which they are considered; II. that Staff Members are aware of and fulfil their information security responsibilities; and III. to protect the Organisation's interests as part of the off-boarding employment process.

5.1 Pre-employment screening

Control	To undertake background verification checks on all candidates for employment in accordance with relevant laws, regulations and ethics that are at all times proportional to our business requirements, the potential information security risks associated with the specific position and perceived risks.

The Organisation will undertake verification checks on all candidates for employment in accordance with relevant laws and regulations. Pre-employment verification procedures will include, to the extent such action would not involve a breach of relevant privacy or employment legislation:

- verification of the applicant's identity;
- review of character references;
- verification of the applicant's curriculum vitae;
- confirmation of claimed academic and professional qualifications; and
- review of criminal history,

for the purposes of confirming that the applicant has the necessary competence to perform the advertised position and ensuring that the individual can be trusted to take on the position.

Where a position, either on initial appointment or on promotion, involves the applicant holding a position as an Information Processing Staff Member, Information Technology Staff Member, a management position or other position that involves access to processing facilities, more detailed verifications may be undertaken by the Organisation at the discretion of Human Resources.

Human Resources must collect and handle any information arising out of the pre-employment verification procedures outlined above in accordance with all relevant privacy and employment legislation.

5.2 Terms and conditions of employment

Control	To clearly state information security responsibilities within contractual agreements with Staff Members.

The Organisation will clearly state the information security obligations of the individual Staff Member in all contractual agreements and provide that individuals meet those information security obligations by including any or all of the following contractual obligations:

- that all Staff Members are required to comply with this Policy as a primary term of employment, including (where reasonably necessary) specific reference to particular sections of this Policy that the Staff Member must comply with in the performance of their position;
- that all Staff Members who are given access to confidential information are required to sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities, or that such terms are included within their employment agreement; and
- that Staff Members are expected to comply with all relevant copyright, privacy and other applicable laws.

The Organisation will advise Staff Members that the failure to comply with these obligations and this Policy may result in disciplinary action up to and including termination of employment or contractor status.

5.3 Management responsibilities

Control	To ensure that management effectively and actively requires all Staff Members to apply information security in accordance with this Policy.

The Organisation must ensure that Staff Members:

- are properly briefed on and inducted into their information security roles and responsibilities prior to being granted access to confidential information or information systems;
- are provided with guidelines stating the information security expectations of their role within the Organisation;
- are motivated to fulfil the Organisation's information security obligations;
- achieve a level of awareness on information security relevant to their roles and responsibilities within the Organisation;
- conform to the terms and conditions of employment, which includes compliance with this Policy;

- continue to have the appropriate skills and qualifications to fulfil their role; and
- are provided regular awareness, education and training, as further outlined in section 5.4 below.

In the event that you are aware of a violation of this Policy or believe there to be ongoing conduct or practices that are in breach of this Policy, you may contact the Organisation's anonymous whistle-blower line via **WAFC Whistle-blower Policy Partner (WAFC Integrity Unit until Partner is confirmed)**. A Staff Member contacting the Whistle-blower Line who has acted in good faith and who has not themselves engaged in serious misconduct or improper conduct will not be treated adversely by the Organisation because they made the report.

5.4 Information security awareness, education and training

Control	To provide adequate and appropriate awareness education, training and regular updates in this Policy, the Privacy Policy and any other relevant policies or organisations to all Staff Members.

The Organisation will undertake regular education and awareness programs on a annual basis to ensure that Staff Members are able to comply with their obligations under this Policy.

As outlined at section 5.2 above, awareness of information security obligations is a key part of every Staff Member's induction program. This program will include fundamental awareness, education and training in this Policy, with particular focus on areas that relate directly to that Staff Member's position. Where a Staff Member is given alternate or additional duties and functions, the Organisation must provide further education and training where reasonably necessary.

Additionally, the Organisation will make available at all times, individual learning modules that may be completed by Staff Members at their own discretion, or as directed by the Information Security Officer, to further promote compliance with this Policy.

5.5 Disciplinary process

Control	To establish a formal and communicated disciplinary process designed to address non-compliance with this Policy.

The Organisation will investigate any alleged or expected breaches of this Policy and determine whether a breach has occurred. In the event a Staff Member is found to have breached this Policy, they may be disciplined. Any disciplinary measures imposed by the Organisation will be appropriate to the severity of the offence and may include:

- verbal or written warnings;
- additional education or training;
- demotion or redeployment; or
- termination of employment.

In deciding the appropriate corrective or disciplinary action, the Organisation may consider the seriousness of the infraction, the circumstances surrounding the matter and the Staff Member's previous record. However, nothing in this Policy limits or restricts the Organisation from taking any action available to it at law.

5.6 Termination or change of employment responsibilities

Control	To maintain adequate post-employment information security obligations, ensure that those responsibilities and duties remain valid and are adequately communicated to employees and, where relevant, contractors.

In certain circumstances, a Staff Member's information security, privacy or confidentiality obligations may continue beyond the end of their employment or contractual agreement. Where applicable, the Organisation will communicate on-going responsibilities and obligations to former Staff Member's during the off-boarding process. Staff Members should note that a failure to comply with these on-going obligations may constitute a breach of their employment contract or contractual agreement and the Organisation may enforce those obligations, in its discretion.

6 DATA SECURITY

6.1 Asset Management

Objective	The purpose of this sub-section is: I. to identify organisations assets and define appropriate protection responsibilities, 6.1(a) to (d); II. to ensure that information assets receive an appropriate level of protection in accordance with their importance to the organisation, 6.1(e) to (g); and III. to prevent unauthorised disclosure, modification, removal or destruction of information stored on media, 6.1(h) to (j).

(a) Inventory of assets

Control	To identify the Organisation's assets that are associated with information and information processes and establish and maintain an inventory of these assets.

The Organisation maintains centralised inventories of information held by the Organisation for the purposes of recording and monitoring our information asset position (**Inventory**). The Organisation must ensure that Inventories are accurate, up-to-date, consistent and aligned with other inventories, where applicable.

The Inventory is used to track our information assets through the lifecycle of information. The Inventory records relevant actions in relation to that information's creation, processing, storage, transmission, deletion and destruction.

(b) Ownership of assets

Control	To ensure that all information assets are allocated to an individual for ownership.

The Organisation will assign an Information Processing Staff-member as an 'owner' of a particular information asset (**Owner**). Generally, the Owner will be the Information Processing Staff-member who created the information.

An asset Owner is responsible for:

- ensuring that information assets are inventoried pursuant to section 6.1(a) above;
- ensuring that information assets are appropriately classified pursuant to section 1.1(a) below;
- ensuring that information assets are assigned necessary protections;

- defining and periodically reviewing access restrictions and classifications to important assets, taking into account applicable access control policies; and

- ensuring proper handling when the information asset is deleted or destroyed.

With the prior authorisation of the Information Security Officer, Owners may delegate routine tasks to other Information Processing Staff, General Staff or other Staff Members, however the obligations outlined in this section remain the responsibility of the Owner at all times.

(c) **Acceptable use of assets**

Control	To identify, document and implement rules for the acceptable use of information assets and information processing facilities.

All Staff Members and external third parties subject to this Policy are expected to use the Organisation's information assets in accordance with directions from senior management and other applicable senior Staff Members, the WAFC IT Acceptable Usage Policy, IT Mobile & Laptop Policy, Code of Conduct and any other relevant controls, policies or procedures.

(d) **Return of assets**

Control	To ensure that all Staff Members and external users return all of the Organisation's information assets upon termination of their employment, contract or agreement.

Prior to, or as soon as practicable after, termination of employment or a contract or agreement with external third parties, individuals subject to this Policy must:

- return all previously issued physical and electronic information assets owned by or entrusted to the Organisation, this may include physical files and forms, laptops, portable hard drives, portable media and any other physical or electronic information storage device controlled by the individual;

- in cases where an individual has been permitted to use personal equipment or hardware, such equipment and hardware must be provided to the Organisation to ensure that all relevant information is transferred to the Organisation and securely erased; and

- in circumstances where an individual has knowledge or expertise that is important to the Organisation's ongoing operations, steps will be taken to document and transfer that information to the Organisation where possible.

(e) Classification of information

Control	To classify information held by the Organisation in light of legal requirements, value and sensitivity to unauthorised disclosure or modification.

The Organisation implements an information asset classification scheme which includes four distinct levels of data sensitivity, as outlined below:

Level 1	Disclosure of the information asset would not cause harm to the Organisation.
Level 2	Disclosure may cause minor operational inconvenience or minor embarrassment.
Level 3	Disclosure may have a significant short-term impact on operations or tactical objectives.
Level 4	Disclosure may have a serious impact on long-term strategic objectives or may put the survival of the Organisation at risk.

Additionally, the Organisation also classifies information assets with reference to privacy obligations, as outlined below:

Non-PI	The information asset is not, and is not expected to be, personal information.
Potential-PI	The information asset is not personal information but may potentially be personal information at a later point in time when combined with or cross referenced against other available personal information.
PI	The information asset is personal information. Refer to section 9.1 for the definition of personal information.
SI	The information asset is sensitive information. Refer to section 9.1 (c) for the definition of sensitive information.

For example, an Owner may determine that an information asset may cause minor embarrassment to the Organisation if disclosed. Additionally, the information asset contains personal information, notably a member's registration details. Such information would be classified as Level 2 – PI.

The classification scheme outlined above (**Classification Scheme**) is intended to provide a concise indication of how sensitive, confidential or critical information is. By grouping information based on its Classification Scheme value, the Organisation can implement class-based security and information processing procedures which reduces the Organisation's risk profile and limits administrative burden.

Additionally, the Organisation notes that the sensitivity, confidentiality or criticality of a particular information asset may change over time. Accordingly, Owners are expected to re-classify information assets in accordance with the Classification Scheme on a periodic basis or whenever there is a distinct change in factors which require a change to the information's classification in order to ensure that information is up to date and accurately classified.

(f) **Labelling of information**

Control	To implement an appropriate labelling procedure for the Organisation's information assets.

In order to ensure that the Organisation's information assets are clearly labelled, accessible and defined, Owners are expected to secure information assets in accordance with the Classification Scheme. Owners must identify information assets:

- electronically by utilising the relevant and appropriate SharePoint folder and ensuring the appropriate level of security is in place giving consideration to 6.1 (e) ; and
- physically by utilising the WAFC IT Asset label naming convention and recording the asset serial number on the asset list.

(g) **Handling of assets**

Control	To develop and implement information handling procedures.

In order to ensure that information assets are provided adequate security and protections commensurate with their classification, the Organisation may impose restrictions limiting access to particular pieces or classes of information assets.

The Information Security Officer or the Owner (with the prior authorisation of the Information Security Officer), may implement access restrictions or additional security measures on individual information assets or classes of information assets.

Where handling restrictions have been imposed pursuant to this section, only those Staff Members or classes of Staff Members authorised to access, use or disclose that information asset may handle that asset.

The Information Security Officer must maintain, or provide for the maintenance of, a record of authorised Staff Members which may be cross-referenced or audited from time to time to ensure compliance with this section.

(h) **Management of removable media**

Control	To implement procedures managing media removal.

The Organisation recognises that removable media and general media storage devices represent a key information security risk to the Organisation if inadequately managed. In order to ensure that we do not suffer a data breach or the loss, misuse or destruction of information, the Organisation implements the following procedures:

- all media must be stored in safe, secure environments in accordance with manufacture specifications where relevant;
- where no longer required, all re-usable media devices that will be removed from the Organisation must be made unrecoverable and disposed of in accordance with section 6.1(i) below;
- the use of removable media devices will only be permitted where it is in our best interests to do so;
- where practical, the Organisation will restrict the removal of media devices from our premises and, if media must be removed, we will record the removal of media devices by our Staff Members;
- all portable or removable media must be subject to cryptographic encryption where reasonable; and
- where media contains valuable data necessary for the Organisation's ongoing business operations, back-ups or duplicate media storage devices will be maintained.

(i) **Disposal of media**

Control	To ensure that media is adequately disposed of when no longer required.

In order to maintain the Organisation's information security and reduce the risk of a data loss or breach, we implement the following procedures for the secure disposal of media containing information assets:

- physical storage devices, such as paper files or media discs should be disposed of securely by shredding or incineration; and
- electronic storage devices should not be disposed of without erasing information from the electronic storage device and ensuring that all information on the device is unrecoverable.

Information Technology Staff are required to maintain a record of media disposed of, including a summary of the information asset contained on the media where practical,

to ensure that audits or reviews of information asset practices may be undertaken in accordance with this Policy.

(j) **Physical media transfer**

Control	To ensure that media containing information is adequately protected against unauthorised access, misuse or corruption during transport.

Where it is necessary to transfer information assets via the physical transfer of portable media, the Organisation implements the following protocols to protect media containing information assets during transport:

- portable media devices may only be transported via a registered courier or Staff Member;
- during transfer, portable media devices must be stored in packaging sufficient to protect its contents from physical damage which may occur during transport; and
- the Organisation will keep a record of the contents of portable media devices, purpose of transfer, time of transfer, transfer custodians and receipt of collection at the transfer destination.

6.2 Access Control

Objective	The purpose of this sub-section is: I. to limit access to information and information processing facilities, 6.2(a); II. to ensure authorised user access and to prevent unauthorised access to systems and services, 6.2(b) to (e); III. to make users accountable for safeguarding their authentication information, 6.2(f) to (h); and IV. to prevent unauthorised access to systems and applications, 6.2(i) to (l).

(a) **Access to networks and network services**

Control	To ensure that users are only provided with access to the network and network services that they are authorised to use.

The Organisation will take all necessary steps to limit Staff Member access to networks and network services only to the extent reasonably necessary for Staff Members to fulfil their role within the Organisation.

(b) **User registration and de-registration**

Control	To develop a formal user registration and de-registration process that governs user access rights.

Information Processing Staff and all other Staff Members with access to the Organisation's information processing systems will be assigned a unique user identification number (**User ID**). Staff Members are prohibited from using joint or shared User IDs.

The Organisation will:

- use User IDs to link Information Processing Staff and other Staff Members to their actions and activities on the Organisation's information processing systems; and
- review User ID logs to hold Staff Members responsible for misuse of information processing systems or non-compliance with this Policy.

The Organisation will immediately disable the User ID of any Staff Member who has left the Organisation or is no longer authorised to access the Organisation's information processing systems.

(c) **User access provisioning**

Control	To develop formal user access provisions that govern the assignment or revocation of access rights for users to the Organisation's systems and services.

The Organisation will manage Staff Member access and authorisation rights by assigning or revoking user privileges to User IDs on a specific or class basis. Access and authorisation rights are assigned by the Organisation in accordance with the Access Control Policy.

The Organisation maintains a central register of access and authorisation rights attributed to User IDs and will periodically review these rights from time to time.

(d) **Management of privileged access rights**

Control	To restrict and control the allocation and use of privileged access rights.

Access to and authorisation to use information processing systems that contain substantially sensitive, confidential or critical information will be managed in accordance with paragraph (a) above, however privileged access will generally be restricted on a need-to-know, need-to-use and event-by-event basis.

The Organisation may impose additional requirements on privileged User IDs, including but not limited to set expiration dates and two-factor authentication protocols.

Staff Members with privileged User IDs are strictly prohibited from sharing privileged access and authorisation rights with any other Staff Members. Inappropriate use of privileged User IDs is a major contributory factor to failures or breaches of the Organisation's information security system and is a serious breach of this Policy.

(e) **Review of user access rights**

Control	To review ongoing access rights on a regular basis and ensure that access rights are removed upon termination of employment or external party user contracts and agreements

In order to ensure that User ID access rights are accurate, appropriate and compliant with this Policy, the Organisation will:

- review access rights on a yearly basis and after any changes, such as promotion, demotion or termination of employment;
- review and re-allocate access rights when Staff Members move from one role to another within the Organisation;
- ensure that the access rights of all Staff Members and third parties is removed upon termination of employment or third-party contracts and agreements; and
- record all changes to access rights for periodic review and audit.

(f) **Management of secret authentication information of users**

Control	To control the allocation of secret authentication information through a formal management process.

The Organisation will provide all Staff Members and relevant third parties a temporary secure password assigned to their User ID prior to being granted access to the Organisation's information systems. User ID holders must change the temporary secure password provided by the Organisation to a unique, secret authentication password for future use of the Organisation's information system (**User Password**).

(g) **Use of secret authentication information**

Control	To require users to follow the Organisation's secret authentication information practices.

All Staff Members and third parties granted a User Password must:

- keep their User Password confidential and not disclose it to any other person;
- avoid keeping a record of their User Password in any format;
- change their User Password if they believe or reasonably suspect that there has been any possible compromise;
- not share their User Password with anyone;
- not use the same password for business and personal purposes; and
- at all times, including when changing their User Password, maintain a User Password that:
    - is at least ten characters long;
    - contains at least one capital letter, one alphabetical character, one numerical character and one symbol; and
    - is easy to remember, not based on anything that could be easily guessed and free of consecutive identical numeric or alphabetical characters.

(h) **Password management system**

Control	To ensure password quality by requiring interactive password management systems.

The Organisation's User Password management system will:

- enforce a choice of quality passwords in accordance with this Policy;
- enforce regular password changes as reasonably necessary;
- not display passwords on the screen when being entered; and
- store and transmit passwords in protected form.

(i) **Information access restriction**

Control	To restrict access to information and application systems in accordance with the Organisation's access control policy.

The Organisation will restrict any Staff Member or third party who is not authorised in accordance with the Access Control Policy from accessing our information and application systems by requiring physical or electronic access controls, including but not limited to User Passwords.

(j) **Secure log-on procedures**

Control	To control access to systems and applications by a secure log-on procedure in line with the Organisation's access control policy.

In order to ensure there is no unauthorised access, the Organisation's information systems and application system log on procedures include the following safeguards:

- system or application identifiers and data will not be displayed until log-on procedures have been completed;
- information systems and application systems will display general warnings that systems should only be accessed by authorised users;
- log-on validation will only occur following completion of all necessary access controls;
- systems and applications will be protected from brute force log-on attempts;
- incorrect and unsuccessful log-on attempts will be recorded in a register, recording the relevant User ID and the date and time of attempt. The Information Technology Manager will review unsuccessful log-on attempts on an ongoing basis;
- log-on pages will not display passwords as they are being entered;
- passwords will not be transmitted in clear text over the network; and
- inactive information or application systems will terminate after a period of inactivity of 15 minutes.

(k) **Use of privileged utility programs**

Control	To restrict and control the use of any utility programs that are capable of overriding the Organisation's systems and application controls.

Utility programs that may be capable of overriding system and application control will be restricted to use by specific authorised users. The Organisation will ensure that:

- use of utility programs is limited to the minimum practical number of trusted, authorised users;
- utility program users will need to follow identification, authentication and authorisation procedures; and
- the use of all utility programs will be logged and reviewed for misuse by the Information Technology Manager and during relevant audit procedures.

(l) **Access control to program source code**

Control	To restrict access to program source codes.

Access to program source code and associated items will be strictly prohibited to prevent the introduction of unauthorised functionality, to avoid unintentional changes and to maintain the confidentiality of valuable intellectual property (where relevant). The Organisation ensures that:

- only specific authorised Staff Members are given access to program source libraries;
- program source libraries are managed according to procedures established by the Information Technology Manager;
- program listings are held in a secure environment;
- audit logs of access to program source libraries are retained and reviewed for misuse by the Information Technology Manager and during relevant audit procedures; and
- maintenance and copying of program source libraries is subject to strict control procedures.

6.3 Mobile & Remote Working

Objective	The purpose of this sub-section is to ensure the security of teleworking and mobile device use within the Organisation.

(a) **Mobile device policy**

Control	To adopt a policy and supporting security measures to manage the risks introduced by using mobile devices.

Staff Members are expected to take special care when using mobile devices to ensure that the Organisation's information assets are not compromised.

The Organisation expects that all Staff Members will comply with the WAFC IT Mobile & Laptop Policy at all times.

(b) **Remote Working policy**

Control	To implement a policy and supporting security measures to protect information accessed, processed or stored at teleworking sites.

'Remote Working' refers to all forms of work outside of the office, including non-traditional work environments, such as telecommuting, remote access workplaces, home workplaces or virtual workplaces (**Remote Working**).

To the extent any Staff Members are engaged in Remote Working, the Organisation expects that Staff Members must comply with the WAFC Flexible Work Policy at all times.

7 PHYSICAL SECURITY

7.1 Secure Areas

Objective	The purpose of this sub-section is to prevent unauthorised access, damage and interference to our information and information processing facilities.

(a) **Physical security perimeter**

Control	To define and implement security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

The Organisation implements the following physical security perimeters:

- when unattended, our office premises remain locked and alarmed to exclude unauthorised entry;
- at all times access to our office premises is restricted;
- at all times external walls and roofs are of sound construction free of gaps and breaks and windows are fitted with locks ensure adequate physical security; and
- video recording devices are installed to review any access to WAFC fixed assets (server room) covered under this policy.

(b) **Physical entry controls**

Control	To limit access to secure areas with appropriate entry controls to ensure that only authorised personal may access secure areas.

To ensure that access to our premises is restricted to authorised personnel only, the Organisation implements the following protocols:

- access to areas of our premises where information processing activities occur are restricted to authorised individuals only. Authorised individuals may access these areas by WAFC staff issued FOB;

- access to areas of our premises where information assets are stored are restricted to authorised individuals only. Authorised individuals may access these areas by obtaining permission and key from either WAFC Facilities or IT staff,

  (together, **Secure Areas**).

Any visitors or third party service providers who are required to access Secure Areas must first sign-in prior to obtaining authorisation to enter secure areas. We will provide visitors and third parties with instructions regarding information security and emergency procedures while accessing Secure Areas.

The Organisation will escort visitors and third parties when attending the business. Staff Members are expected to immediately notify security personnel if they encounter unescorted visitors in Secure Areas who are not displaying visible identification.

(c) **Securing offices rooms and facilities**

Control	To design and apply physical security for offices, rooms and facilities.

The Organisation imposes additional restrictions designed to secure offices, rooms and processing facilities from the public by:

- restricting information processing facilities from view of the public where practical at all times;

- configuring information processing facilities to prevent confidential information or activities from being visible or audible from outside; and

- restricting directories and floor-plans referring to information processing facilities.

(d) **Protecting against external and environmental threats**

Control	To design and apply protections against natural disasters, malicious attack or access.

The Organisation's premises have been designed, as far as reasonably practicable, to protect against or reduce the effect of natural disasters or malicious attack or access.

(e) **Working in secure areas**

Control	To design and apply procedures for working in secure areas.

Access to Secure Areas is provided on a 'need-to-know' or 'need-to-access' basis. Secure Area authorisation is only provided to those Staff Members and individuals who need to access the Secure Area.

Where practicable, authorised personnel should not work in Secure Areas alone or unsupervised to reduce the potential safety risk and to prevent opportunities for malicious activities.

(f) **Delivery and loading areas**

Control	To control access points, such as delivery and unloading areas, to limit unauthorised access.

In order to reduce the risk of unauthorised access to the Organisation's premises, we have implemented the following protocols at access points such as delivery and unloading areas:

- access to delivery and loading areas from outside our premises are restricted to identified and authorised persons only;
- our delivery and loading areas allow supplies to be loaded and unloaded without delivery personnel gaining access to Secure Areas;
- incoming materials and supplies are registered and recorded by Staff Members; and
- evidence of tampering with delivery products or otherwise suspicious deliveries must be reported to security personnel.

7.2 Equipment

Objective	The purpose of this sub-section is to prevent loss, damage, theft or compromise of assets and interruption to our operations.

(a) Equipment siting and protection

Control	To ensure that equipment is sited and protected in a manner that reduces risks from environmental threats, hazards and opportunities for unauthorised access.

To protect the Organisation's equipment against environmental hazards and unauthorised access, we implement the following protocols:

- information processing facilities and storage facilities are secured to avoid unauthorised access; and
- temperature controls are in place; and
- surge protection and continuous power (UPS) devices for all servers.

(b) Supporting utilities

Control	To protect equipment from power failures and other disruptions caused by failures in supporting utilities.

The Organisation protects its supporting utilities (electricity, telecommunications, water, gas, sewage, ventilation and air conditions, together **Supporting Utilities**) from misuse by:

- ensuring that Supporting Utilities conform to manufacturer specifications;
- engaging independent service providers to inspect and review Supporting Utilities on a periodic basis;
- considering potential Supporting Utilities expansion to meet business growth periodically and when reasonably necessary;
- where practicable, alarming Supporting Utilities to detect malfunctions; and
- providing for automatic responses, such as automatic lighting or valve shutdowns to water, gas or other utilities during emergency situations where necessary.

(c) **Cabling security**

Control	To ensure that power and communications cabling carrying data or supporting information services is protected from interception, interference or damage.

To protect the Organisation's cabling from misuse, interference or damage, we ensure that:

- power and telecommunication lines are provided adequate protection;
- power cabling is segregated from telecommunications or alternate cables to reduce the likelihood of interference; and
- access to panels and cable rooms is restricted to authorised users only.

(d) **Equipment maintenance**

Control	To maintain equipment correctly to ensure its continued availability and integrity.

The Organisation implements the following protocols regarding equipment maintenance:

- all equipment must be maintained in accordance with the supplier or manufacturer's recommended service intervals and specifications;
- equipment repairs and service may only be undertaken by authorised maintenance personnel;
- maintenance personnel must maintain records of suspected or actual equipment faults; and
- before recommissioning equipment that had been removed for maintenance, maintenance personnel will inspect and test equipment to ensure that it has not been tampered with and does not malfunction.

(e) **Removal of assets**

Control	To restrict the removal of equipment, information or software off our premises without prior authorisation.

Equipment may not be removed from the Organisation's premises other than in accordance with applicable policy, such as the Organisation's Flexible Work Policy, or with the prior authorisation of the Information Security Officer or the Information Technology Manager.

When authorising equipment removal, the Information Security Officer and the Information Technology Manager must:

- implement time limits that establish specific return dates; and
- where necessary and appropriate, maintain a record of who has removed equipment and when equipment is removed from and returned to our premises.

(f) **Security of equipment and assets off-premises**

Control	To apply security measures to any assets that are taken off-site, taking into account the different risks of working outside our premises.

Staff Members are responsible for ensuring that equipment which is taken off the Organisation's premises is secure and protected by:

- ensuring that equipment is not left unattended in public places; and
- complying with manufacturer instructions at all times when using or storing equipment.

(g) **Secure disposal or re-use of equipment**

Control	To verify all storage media prior to disposal or re-use to ensure that sensitive data, licensed software or other critical information has been removed or securely overwritten.

Prior to disposal or re-use of equipment, equipment must be verified by Information Technology Staff to ensure that the equipment does not contain any information assets. Where equipment does contain information assets, or a Staff Member reasonably expects it may contain information assets, it must be disposed of in accordance with section 6.1(i) above.

(h) **Unattended user equipment**

Control	To ensure that unattended equipment has appropriate protections applied.

In order to ensure that unattended equipment is protected from misuse or unauthorised access, Staff Members are expected to:

- log-off from applications or network services when no longer in use; and
- ensure that computers and mobile devices are secured by a key lock, password or equivalent control.

(i) **Clear desk and clear screen policy**

Control	To adopt and enforce a clear desk and clear screen policy to protect papers, storage media and processing systems from unauthorised use.

Staff Members are expected to keep personal workstations secure from misuse or unauthorised access by:

- ensuring that sensitive or critical business information (being information assets classified as Level 3 or Level 4) in physical storage is kept secured in a locked filing cabinet or desk when not required; and
- leaving computers and terminals logged off when not in use.

8 THIRD PARTY SECURITY

8.1 Information security in third party relationships

Objective	The purpose of this sub-section is to ensure our assets that are accessible by suppliers are protected.

(a) **Information security policy for third party relationships**

Control	To agree and document general information security requirements with third parties to mitigate risks associated with third party access to information or information processing systems.

The Organisation identifies general information security protocols necessary to protect our information assets pursuant to this Policy prior to providing any third party access to our information systems.

(b) **Addressing security within third party agreements**

Control	To establish and agree relevant information security requirements with third parties

The Organisation must enter into an agreement with any third party who may have access to our information assets that provides:

- a description of the information to be provided and the methods of accessing the information;
- the classification of the information in accordance with section 1.1(a) above;
- the legal and regulatory requirements, including privacy, intellectual property and data protection laws that may apply to the information and how the third party must ensure that they are met;
- obligations for the third party to implement an agreed set of controls drawn from this Policy to protect our information assets;
- rules regarding the acceptable use of information;
- a list, or criteria to establish a list, of third party personnel authorised to access our information systems;
- incident management requirements and procedures;
- where relevant and practical, training and awareness programs that the third party must complete;
- screening requirements for authorised personnel;
- a right to audit the third party's supplier processes and controls; and
- defect and conflict resolution procedures (as applicable),

(a **Third-Party Agreement**).

(c) **Information and communication technology supply chain**

Control	To require third parties to address relevant information security risks during the product or services supply chain.

In order to ensure that the Organisation's information assets are protected from misuse or unauthorised access throughout the goods or services supply chain, we may require third parties, where practical and relevant, to provide supply chain security by requiring sub-contractors and suppliers comply with the same information security protocols included in the Third-Party Agreement.

8.2 Third party service delivery management

Objective	The purpose of this sub-section is to maintain an agreed level of information security and service delivery in line with third party agreements.

(a) Monitoring and review of third-party services

Control	To provide for regular monitoring, reviewing and auditing of third-party service delivery.

In order to ensure that the information security terms and conditions of Third-Party Agreements are being met, the Organisation:

- monitors third party service performance levels to verify adherence to Third Party Agreements;
- conducts ongoing and periodic reviews of information security standards maintained by third parties where permitted under Third Party Agreements;
- commissions the preparation of reports following identified information security incidents occurring to third parties and reviews this information as part of our incident response policy outlined further in section **Error! Reference source not found.** below; and
- resolves and manages any identified problems arising out of the third party relationship.

(b) Managing changes to third party services

Control	To manage changes to third party service provisions, with reference to the importance of business information, systems and processes involved in those service provisions and risk assessments.

From time to time, it may be necessary for the Organisation to improve or amend existing information security policies, procedures and controls imposed to third parties when the critical nature of information assets change, or our standards, systems and processes change which require a re-assessment of risk.

The Organisation will review and, where reasonably necessary, improve or amend information security obligations imposed on third parties in Third Party Agreements where:

- there is a substantial change to the supplier agreement;
- the Organisation implements changes that enhance our service offerings, involve the development of new applications and systems or modify this Policy; or

- the third party implements changes to their services to enhance their network, use new technologies or systems, adopt new products or versions of prior products, develop new tools or environments, transition to new physical locations or facilities, change suppliers or sub-contract to another supplier.

9 PRIVACY

Objective	The purpose of this section is to ensure we comply with our obligations under the Privacy Act when collecting, using, storing and disclosing personal information.

In this section 9, a word or expression defined in the Privacy Act has the meaning given to it in the Privacy Act.

9.1 The *Privacy Act 1988* (Cth)

The West Australian Football Commission is considered to be an organisation, and relevantly an APP Entity, which is subject to the Australian Privacy Principles (**APP**) under the Privacy Act. The Privacy Act imposes a series of obligations and requirements on the Organisation regarding the collection, use, storage and disclosure of personal information.

The definition of 'personal information' is outlined below:

Personal Information	Personal information is any information or an opinion about an identified individual or an individual who is reasonably identifiable. Common examples of personal information include an individual's name, their address, bank account details, and more broadly information about that person such as their habits, trends, performance or views, whether factual or an opinion about that person. What constitutes personal information is not always clear and will vary depending on a variety of circumstances.

Our obligations under the Privacy Act are summarised below.

(a) APP 1 – Open and transparent management of personal information

The Organisation is required to take such steps and implement practices, procedures and systems to ensure that the Organisation comply with the APP and which enable us to deal with enquiries or complaints from individuals regarding the Organisation's handling of their personal information. Additionally, the Organisation is explicitly required to publish and maintain a clearly expressed privacy policy.

The Organisation's privacy policy is published on our website, available here https://www.wafootball.com.au/privacy-policy/. The Organisation will comply with its obligations under APP 1 by operating in accordance with this Policy and our Privacy Policy.

(b) **APP 2 – Anonymity and pseudonymity**

An individual must be given the option, where practicable, to not identify themselves or to use a pseudonym in their interactions with our business.

We may require individuals to identify themselves where we are required by law to deal with individuals who have identified themselves or where it would be impracticable for us to deal with individuals on an anonymous or pseudonymous basis. In most circumstances, it is impractical for people to communicate with the Organisation anonymously, however Staff Members should be aware to allow individuals to correspond anonymously or pseudonymously, particularly if their enquiry does not relate to registration with the AFL or WAFC or membership of a WAFL or WAFLW club.

(c) **APP 3 – Collection of solicited personal information**

The Organisation may only collect personal information that is reasonably necessary for one or more of our functions or activities. Our Privacy Policy outlines the type of information that we generally collect, these include:

Registration or Identity Information	Payment Information	Communication Information
When individuals register, either directly with WAFC or through a third party with which we have a registration sharing relationship, such as the AFL, individuals provide information including their full name, email address, postal address, telephone number, date of birth, occupation, location and such other registration information as may be requested by us or our partners from time to time.	In order to facilitate payments or other financial transactions with us, individuals may provide us with financial information relating to them or another person, which may include bank account details, credit, debit or bank card details or other billing information.	If individuals communicate with us via telephone, email, SMS or online, we may collect information relating to them and any other personal information they choose to provide to us while communicating with us.

Sporting Information	Ticketing Information	Cookie Information
When individuals participate in community football events and organisations, personal information about their performance or participation in such events may be collected by us or our partners.	When individuals purchase tickets through Ticketmaster to an event organised by WAFC, we collect certain limited information from Ticketmaster relating to their attendance at our event.	We use cookies and similar tracking technologies on our website or app in order to track the use of our services and our website or app, and to maintain and improve our services to individuals.

Health Information	Mobile Data Information	Third Party Plug-In Information
In the course of providing our services, individuals may be required to provide us with information about their health, including past or present injuries other medical information. Health information is considered 'sensitive information' and we only collect health information with consent and as reasonably necessary to carry out our services.	Individuals may access or use our services via a mobile device or application. We may collect information about them and their device, such as their IP address, location or device information, and any other information provided by their mobile device.	In some cases, we may have integrated a third-party plugin into our website. The use of such third-party plugins may result in data collection by both our business and the relevant third party. We do not control the information individuals share with third parties via these plugins and such information is not the subject of this Policy.

Other Information
Individuals may provide us information through their participation in product engagement, social media platforms, customer surveys or other sources that are implemented, published or adopted by us.

Whenever reasonable and practical to do so, we will collect personal information about our customers/stakeholders/participants directly from them. However, in some cases we may be required to collect personal information about them from third parties such as through our partners and service providers, including but not limited to the AFL, WAFL or WAFLW clubs, Ticketmaster and Play HQ and Officials HQ or from public sources. Where we collect information from a third party, we will take reasonable steps to ensure that the customer is made aware of the fact and circumstances of that collection. We may also receive information from third parties where the customer has authorised the third party to do so.

We collect this information in order to carry out our business operations in the most professional and efficient manner possible.

The Privacy Act provides additional protection to sensitive information. Sensitive information is defined below:

Sensitive Information	Sensitive information is a subset of personal information defined as: (a) information or an opinion (that is also personal information) about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record; (b) health information about an individual; (c) genetic information (that is not otherwise health information); (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

The Organisation may only collect sensitive information with our customers' consent unless an exception applies. Generally, we will not collect information from our customers that is considered sensitive information. If there is any cause to collect sensitive information from our customers, we must ensure that consent is obtained prior to collection.

In addition, the Organisation may only collect personal information by lawful and fair means. We do not engage in unlawful or unfair collection of personal information. As outlined above, we will generally collect information directly from our customers. In the event we need to collect personal information from third parties, our customers are made aware of that collection via our Privacy Policy. Prior to collecting any information that may be personal information from customers, we must ensure that the customer has been provided with a data collection notice, or alternatively has been directed to view and consider our Privacy Policy.

(d) APP 4 – Dealing with unsolicited information

If the Organisation receives unsolicited personal information, for example – identity information included in an unsolicited enquiry, we must determine within a reasonable time period whether we could have collected the information if we had solicited the information.

Any unsolicited information received by the Organisation must be reviewed against the information types we generally collect, as outlined at paragraph 9.1(c) above. If the information is not necessary for our business operations or functions, or if the unsolicited information is sensitive information, we must ensure that the information is destroyed or de-identified immediately.

(e) **APP 5 – Notification of the collection of personal information**

We are required to identify ourselves to our customers when collecting personal information and notify them of the circumstances of collection and of specific information they should be aware of. The matters that we must notify customers of upon collection include:

- our contact information;
- the fact and circumstances of collection;
- whether the collection is required or authorised by law;
- the purposes of collection;
- the consequences if information is not collected;
- where we may disclose the information;
- information about our privacy policy; and
- if we are likely to disclose the information to overseas recipients

In order to comply with our notification obligations, we provide our customers with a privacy collection notice when collecting personal information. In the event we are required to collect information in alternative circumstances, customers should be directed to our Privacy Policy prior to collecting personal information.

We maintain various data collection notices that are to be used:

- Customers, Vendors & Suppliers
- Job Applicants
- Registered Users
- WAFC Website

Information Processing Staff must ensure that provision of these collection notices is provided in accordance with this policy where practicable at all times.

(f) APP 6 – Use or disclosure of personal information

The Privacy Act provides that the Organisation may only use or disclose personal information for the purpose the information was collected and may only use the information for secondary purposes where the individual has consented to such use or an exception applies.

We collect our customers' personal information for the following purposes:

- to administer and manage Western Australian football participation
- to set-up and update your registration details with us
- to comply with legal obligations
- to contact individuals regarding our services
- to deliver targeted marketing materials regarding Western Australian football and offers we believe may be of interest to individuals
- to co-ordinate or confirm membership details of WAFL, WAFLW & AFL clubs
- to collect fees and payments owing to us
- to resolve disputes
- to respond to enquiries and concerns
- to otherwise provide services to people involved in football in Western Australia
- to provide member and participant support
- for insurance purposes
- to advertise our services to the products and services of third parties

We advise our customers of these collection purposes in our Privacy Policy. Additionally, when we collect personal information, we will generally provide a privacy collection notice that specifies the specific purposes for collection. Our Privacy Policy and any privacy collection notice outlines that we may use their personal information for secondary purposes connected to the purposes outlined above. In order to ensure that we may use the personal information for the purposes outlined above, Information Processing Staff must ensure that our customers have consented to collection in accordance with our Privacy Policy when they collect personal information.

In order to comply with the Privacy Act, the Organisation may only use personal information for the purposes outlined above and for secondary purposes related to those purposes (however caution should be placed on using sensitive information for secondary purposes).

(g) APP 7 – Direct marketing

The Privacy Act prohibits the Organisation from using or disclosing personal information for the purposes of direct marketing unless an exception applies. We may use personal information for the purposes of direct marketing:

- if we have collected the information ourselves – where our customer would reasonably expect us to use the information for the purposes of direct marketing; or

- if the information is collected from a third party (as opposed to from the customer directly) or if the individual would not expect the organisation to use the information for direct marketing purposes – where the individual has given their consent to do so, or it would be impracticable to obtain consent and they would otherwise reasonably expect us to use their information for direct marketing purposes.

However, pursuant to the *Spam Act 2003* (Cth) (**Spam Act**), the Organisation is prohibited from sending direct marketing emails to customers without obtaining express (or, in certain circumstances implied) consent. In order to comply with the Spam Act the Organisation *does not engage* in direct marketing without obtaining the customers' express and active consent to do so.

All direct marketing is required to include a functional 'unsubscribe' function. In the event an individual has exercised this function, we must cease sending them direct marketing as soon as possible.

(h) **APP 8 – Cross-border disclosure of personal information**

In the event that personal information must be disclosed to overseas entities, the Organisation must take reasonable steps to ensure that the international recipient does not breach the APPs when dealing with transferred personal information. However, this requirement does not apply where:

- the international recipient is subject to substantially similar privacy obligations as those contained in the APPs and the Australian individual can take action to enforce those data protection laws; or

- where the individual has been expressly informed of the disclosure and the individual consents to such disclosure.

While the term 'disclosure' is not explicitly defined in the Privacy Act, it is understood to mean the act of making personal information accessible or visible to others outside the Organisation while also releasing the subsequent handling of the information from the Organisation's control. The Organisation may disclose information when we send data to third party service providers in connection with a data sharing agreement, or when we use third party data storage suppliers.

We generally do not send personal information overseas and will prioritise third party data processing arrangements that do not require overseas disclosure of personal information.

In the event that we are required to disclosure personal information to overseas recipients, the Organisation will ensure that we have obtained individual consent to do so via a data collection notice.

Where we have failed to obtain consent prior to disclosure, or obtaining consent is impractical in the circumstances, we must ensure that we only disclose personal information to jurisdictions that have substantially similar privacy obligations to Australia and where our customers can take action in that jurisdiction to enforce those obligations. Authorisation from the Organisation's Information Security Officer is

required prior to disclosing information to third parties overseas without the individual's consent.

(i) **APP 9 – Adoption, use or disclosure of government related identifiers**

The Privacy Act prohibits the Organisation from adopting a government related identifier, such as a driver's licence, Medicare or passport number, as its own identifier of an individual unless an exception applies.

The term 'adoption' is not defined in the Privacy Act, however the OAIC's guidance establishes that the 'adoption' means the organisation of personal information held by an entity with reference to a government related identifier. The Organisation organises the personal information we hold about our customers via reference to their registered email address (**Registration ID**) and not via a government related identifier. The collection, use and storage of personal information must be referenced against Registration Numbers and not against any government related identifiers.

In addition, the Organisation must not use or disclose a government related identifier unless a specified exception applies.

(j) **APP 10 – Quality of personal information**

The Organisation is obligated to take such steps (if any) as are reasonable in the circumstances to ensure that the personal information we collect is accurate up to date and complete.

In order to meet this obligation:

- Information Processing Staff should, where practicable, provide individuals the opportunity to update their personal information when interacting with individuals from time to time; and

- the Information Security Officer will develop and implement processes and procedures to review, update and ensure that personal information stored by the Organisation is accurate (including identifying any information that should be deleted or de-identified as appropriate).

(k) **APP 11 – Security of personal information**

The Organisation must take reasonable steps to protect personal information we hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

This Policy applies to the management of information generally and includes the management of personal information. By implementing and complying with this Policy, the Organisation is taken to be taking reasonable steps to protect our customer's personal information. You must ensure that you comply with this Policy at all times when dealing with personal information.

Additionally, when we no longer need our customer's personal information we must take reasonable steps to destroy the information or ensure that it is de-identified.

(l) **APP 12 & 13 – Access to, and correction of, personal information**

Pursuant to APP 12 and APP 13, the Organisation must, when requested to do so by our customers:

- provide that customer access to the personal information we hold about them; and
- correct that customer's personal information if the information we hold is incorrect, incomplete, misleading or out of date.

Our Privacy Policy provides our customers the option to contact us regarding access to or correction of personal information. The Information Security Officer will address, or delegate, all customer requests in order to manage our customers' rights under the Privacy Policy.

10 DATA BREACH MANAGEMENT

10.1 Overview

Objective	The purpose of this section is to ensure the Organisation complies with its obligations under the Privacy Act with respect to data breaches.

This section establishes a data breach response plan designed to respond to security breaches that lead to the loss, destruction, alteration or unauthorised disclosure or access to personal information (**Data Breach Response Plan**). The Data Breach Response Plan should be read in conjunction with, and is designed to operate alongside, the Organisation's incident management obligations.

In this section 10, a word or expression defined in the Privacy Act has the meaning given to it in the Privacy Act.

10.2 Notifiable Data Breach Scheme

The Notifiable Data Breach Scheme is established under Part IIIC of the Privacy Act (**NDB Scheme**). The NDB Scheme provides that a 'data breach' occurs where personal information held by an organisation is lost or subject to unauthorised access or disclosure. The Organisation has obligations to notify individuals and the OAIC where an 'eligible data breach' occurs, which is defined as:

Eligible Data Breach	An eligible data breach occurs where: (a) there is unauthorised access to, or disclosure of personal information held by the Organisation (or information is lost in circumstances where unauthorised access or disclosure is likely to occur). In other words, a 'data breach' has occurred;

(b) the data breach is likely to result in serious harm to any of the individuals to whom the personal information relates; and

(c) the Organisation has been unable to prevent the likely risk of serious harm with remedial action.

If it is unclear whether a data breach has occurred, but there are reasonable grounds to suspect an eligible data breach, the Organisation must undertake a reasonable and expeditious assessment to determine if an eligible data breach has occurred. In such circumstances, the Organisation must reach a decision on whether an eligible data breach has occurred within 30 days of identifying the possible data breach.

If the Organisation determines that an eligible data breach has occurred, the Organisation must prepare a statement (**Data Breach Statement**) setting out:

- the Organisation's contact details and the direct contact details of the Information Security Officer;
- a description of the eligible data breach;
- an outline of the personal information concerned or involved in the eligible data breach; and
- recommendations that individuals should take in response to the eligible data breach.

The Organisation must provide the Data Breach Statement to the Privacy Commissioner at the OAIC as soon as reasonably practicable, and to all individuals the subject of the eligible data breach where it is practical to do so.

10.3 Data Breach Team

In the event a data breach has been identified or comes to the attention of the Organisation, the Organisation will establish a team to respond to the breach (**Data Breach Team**). The Data Breach Team will consist of:

Data Breach Response Lead	The Organisation will assign a member of the Organisation's board or an executive manager who will fulfil the role of managing and co-ordinating the overall data breach review and response efforts.
Information Security Officer	The Information Security Officer will ensure that the Data Breach Team complies with the Organisation's obligations under the NDB Scheme and this Policy.
Information Technology Manager	The Information Technology Manager is responsible for co-ordinating the Data Breach Response Plan with the Organisation's incident management protocols and providing information technology assistance.

Relevant Team Manager	In the event the Organisation is able to identify the relevant source of personal information, the Organisation may, where reasonably necessary, assign the lead manager to the department responsible for that personal information to the Data Breach Team in order provide further insight into the types and nature of personal information the subject of the breach and to provide additional relevant insight.
Human Resources	In the event a data breach impacts the Organisation's staff-members, the Organisation will assign Human Resources staff to the Data Breach Team to assess and recommend risk mitigation measures to assist affected Staff Members.
Legal Counsel	Where reasonably necessary, the Organisation will engage external legal counsel to assist the Data Breach Team in complying with their obligations under the NDB Scheme.
Outside Experts	Where reasonably necessary, the Organisation will engage external communications or cyber security experts to assist the Data Breach Team in addressing the data breach.

The Organisation will assign Staff Members or individuals to the Data Breach Team as soon as practicable after identifying a potential or expected data breach and may appoint additional members to the Data Breach Team from time to time.

10.4 Data Breach Response Plan

These procedures may be invoked via a variety of communication channels, including input from customers, third parties, the public, Staff Members or Information Technology Staff. All Staff Members must direct any notices regarding potential data breaches to the Information Technology Manager for assessment and review. Where the Information Technology Manager considers it is reasonably likely that a data breach has or may have occurred, the Information Technology Manager will initiate the Data Breach Response Plan.

Once the Data Breach Response Plan is initiated, the following steps will be followed:

- the Organisation will assign a Data Breach Response Lead who will co-ordinate the remaining Data Breach Team immediately;
- the Information Technology Manager, in consultation with the Information Security Officer where necessary, will immediately prepare an initial brief to the Data Breach Team outlining the nature of the data breach, the type of data involved, the approximate number of records or amounts of data involved, an estimation of the types of individuals affected by the breach, proposed technical remediation plans and identified risk reduction measures; and
- the Data Breach Team will immediately commence necessary and available response measures while simultaneously undertaking further steps as outlined as sub-paragraphs (a) to (c) below.

(a) **Data Breach Review**

Control	To explicitly identify and document the legal risk, severity and scale of the data breach.

The Data Breach Team will undertake all necessary enquiries to:

- identify the scope and extent of the data breach, including a more fulsome report on the type of data involved, number of records or amount of data involved and the types of individuals or customers involved;
- identify any relevant Third Party Agreements where obligations exist to report data breaches;
- identify if the data breach may have extraterritorial scope and whether the Organisation may need to comply with alternate data breach response measures in foreign jurisdictions; and
- track media coverage and devise initial strategies to address adverse coverage.

(b) **Eligible Data Breach Determination**

Control	To determine whether the data breach constitutes an eligible data breach for the purposes of the Privacy Act.

Following completion of the data breach review steps outlined in sub-paragraph (a) above, which must be completed as soon as reasonably practicable, the Data Breach Team must make a reasonable assessment as to whether:

- the data breach is likely to result in 'serious harm' to the individuals effected; and
- if there are any steps the Organisation can take to mitigate that potential harm.

The term 'serious harm' is broadly construed under the Privacy Act to include serious physical, psychological, emotional, economic, financial and reputational harm. When determining whether an individual is likely to suffer serious harm, the Data Breach Team must undertake a holistic assessment of the potential harm an individual may suffer by considering matters such as:

- the type or sensitivity of information involved;
- whether protections or encryptions are applied to protect the information;
- whether those protections or encryptions could be overcome;
- who has or may have access to the information;
- the likelihood those persons would use the information to cause harm to the individual; and

- the nature of harm or other relevant matters.

Where the Data Breach Team considers that a reasonable person would consider it is likely that an individual will suffer serious harm from the data breach, taking into consideration any possible mitigating actions, the Data Breach Team must declare the data breach as an eligible data breach and undertake the briefing and communication activities outlined in sub-paragraph (c) below.

(c) **Briefing and Communications**

Control	To undertake communications and briefing activities necessary to comply with the Privacy Act and additionally where in the best interest of the Organisation.

Where the Data Breach Team considers an eligible data breach has occurred they must ensure that:

- the Data Breach Team briefs the Organisation leadership and other relevant stakeholders on all matters relevant to the eligible data breach;
- contact is established with appropriate third parties, such as insurers, law enforcement and regulatory bodies;
- preparation and publication of a Data Breach Statement is attended to immediately and in any event is provided to the OAIC within 72 hours of identifying an eligible data breach has occurred;
- Staff Member welfare is addressed where relevant;
- customer communication and personal-relations matters are attended to; and
- all other necessary steps are taken to comply with the Privacy Act and to protect or maintain the Organisation's business interests.

10.5 Post Incident

The Data Breach Team must undertake a post-incident review to:

- determine the effectiveness of the Data Breach Response Plan in relation to the specific data breach;
- address any residual issues arising out of the data breach, such as insurance, litigation and regulatory compliance; and
- assess whether the Organisation should implement any amendments to the Data Breach Response Plan moving forward.

11 COMPLIANCE

Objective	The purpose of this section is to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and any other security requirements.

11.1 Identification of applicable legislation and contractual requirements

Control	To explicitly identify, document and periodically update all relevant legislative, statutory, regulatory and contractual requirements regarding information management and to outline our approach to meet these requirements.

All Staff Members are expected to comply with all relevant legislation, regulations, industry codes or contractual obligations at all times (**Compliance Obligations**).

Management staff are expected to be aware of all relevant Compliance Obligations and any update or amendment to those obligations within a reasonable timeframe.

Where directed by management staff, or where the Organisation considers it is reasonably necessary, the Organisation will provide periodic training to Staff Members in order to assist in meeting the Organisation's Compliance Obligations.

11.2 Intellectual property rights

Control	To implement appropriate procedures to ensure compliance with legislative, regulatory, and contractual requirements relating to intellectual property rights and the use of proprietary software.

In order to ensure that the Organisation operates in compliance with intellectual property laws, Staff Members must comply with our Employment Contracts, specifically *Intellectual Property*.

11.3 Protection of records

Control	To protect records from loss, destruction, falsification, unauthorised access and unauthorised release in accordance with legislative, regulatory, contractual and business requirements.

In order to ensure the Organisation's organisational records are maintained in accordance with all relevant record keeping Compliance Obligations and in the best interest of the Organisation, Staff Members must comply with our Code of Conduct.

11.4 Regulation of cryptographic controls

Control	To implement cryptographic controls in compliance with all relevant agreements, legislation and regulations.

Information Technology Staff must ensure that the Organisation operates in compliance with all relevant cryptographic Compliance Obligations at all times.

12 AUDIT & MONITORING

Objective	The purpose of this section is to ensure that information security continues to be implemented and operated in accordance with the Organisation's policies and procedures.

12.1 Independent review of information security

Control	To ensure that the Organisation's approach to managing information security and its implementation is reviewed independently at planned intervals or when significant changes occur.

The Organisation will initiate independent reviews of this Policy to ensure the continuing suitability, adequacy and effectiveness of our approach to managing information security (**Independent Review**). An Independent Review must:

- be undertaken by individuals independent of the area under review and may, where necessary, include outside auditing personnel; and
- be undertaken by individuals with the appropriate skill and experience in information security.

An Independent Review should include an assessment of possible opportunities to improve the Organisation's information security practices or policies and recommend changes where necessary. The results of the Independent Review must be recorded in a report to be provided to management for review.

The Organisation must undertake an Independent Review where:

- a significant event occurs, such as a change in the nature or scope of our activities or information processing systems, a change in best practice procedure or a significant security incident or data breach; and
- in any event, on an annual basis.

In the event that an Independent Review identifies that the Organisation's information security is inadequate or improperly implemented, we must consider all relevant and practicable corrective actions to ensure information security moving forward.

12.2 Compliance with security policies and standards

Control	To provide for the regular review of compliance with information processing and procedures within particular areas of responsibilities by personnel experienced and with authority in those areas to ensure appropriate security policies, standards and other security requirements are maintained.

Managers are expected to undertake an ongoing review of their department's compliance with this Policy from time to time. Where a manager identifies non-compliance with this Policy they must:

- identify the cause of non-compliance;
- evaluate the need for actions to achieve compliance;
- implement appropriate corrective action;
- review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses; and
- record the non-compliance and corrective action taken for further review during the next upcoming Independent Review.

12.3 Technical compliance review

Control	To regularly review information systems for compliance with the Organisation's information security polices and standards.

Information Technology Staff, under co-ordination by the Information Technology Manager, are expected to undertake ongoing reviews of the Organisation's technical systems. In the event Information Technology Staff identify technical errors or insufficiencies they must report to the Information Technology Manager who must:

- review the identified error or insufficiency;
- identify the cause;

- evaluate the need for actions to achieve compliance with this Policy;
- implement appropriate corrective action;
- review the corrective action undertaken to verify its effectiveness and identify any deficiencies or weaknesses; and
- record the non-compliance and corrective action taken for further review during the next upcoming Independent Review.