Contents

1 Policy Statement

1.1 Objectives

The key objectives of the policy are:

- To clearly identify acceptable use of information and information systems.
- Increase security awareness among Officers who use the Association information and information systems
- Clearly inform Officers of what is acceptable use and the consequence of use other than what is permitted
- Improve productivity through efficient and responsible Officers behaviour

1.2 Scope

This policy applies to all officers, consultants, contractors, and outsourced service providers performing work for the Association. It also applies to all information and information system assets owned, leased or outsourced by the Accociation at all its business locations, non-Association sites (including private residences), regardless of format or storage device, and whether shared or allocated to individuals. Information and information systems encompass facilities, technology, application systems and data.

1.3 Ethical Conduct

All activities must be conducted in an ethical and transparent manner and comply with the values, principles, and articles in the Code of Conduct.

Use of the Association information and information system assets must be ethical, efficient, lawful, and economic as defined in the Information Security Policy and the Code of Conduct. All Officers that are in possession of or have access to the Association information or information system assets must take reasonable steps to protect those assets against loss, damage, or destruction. This relates to physical and electronic files, documents, and records, as well as equipment.

Officers have responsibility for maintaining a reasonable level of security over the off-site use of the Association information and information system assets, considering the relevant circumstances and the risks of working outside the Association premises.

2 Acceptable Use

2.1 Introduction

Information and information systems are vital in the Association for decision making, supporting business processes, and delivering our services. Information and information system resources are important and valuable Association assets that must be protected and used appropriately. Significant business benefits arise from managing information and information systems in a structured and formal way, including improving services to the members, competitive edge,

profitability, legal compliance, and commercial image. This in turn supports achievement of the Association objectives.

2.2 Background

The key elements of this policy are the access to information and information system and the acceptable use of the privileges provided by this access. Acceptable use is using resources for business purposes in an efficient, economical, lawful, and ethical manner. The most common security problems related to access and use are:

- Passwords being forgotten, guessed, shared, or misused, insecurely stored
- Confidential information being handled indiscreetly (such as being left on desk or emailed with inadequate precautions) or not being properly classified
- Unauthorized changes being made to computers or the network (such as installing unauthorised equipment or software)
- Use of systems for unreasonable private purposes

The overriding factors that have shaped this policy are:

- The Association has statutory and organisational responsibility to ensure confidentiality, integrity and availability of the Association information and information systems
- Compliance with the Privacy and Personal Information Protection Acts and Workplace Surveillance Act;
- Compliance with State Government directives concerning information security (ISO 27001). This directive has been mandated by the government to protect the government against incidents and attacks on its information, communication and technology systems that could significantly reduce the operational effectiveness of Government.

2.3 User Access and Password Management

All Officers requiring access to Association systems and information will be provided with such access:

- After the Officers have agreed and signed the Association Code of Conduct and User Access Form
- The Business Manager must request access for new Officers and access changes for all Officers
- Business Managers must ensure access is provided on the principle of least possible privilege and need to know basis
- Business Managers must ensure access is removed on Officers departure from the Association

Officers must ensure their passwords are:

- Sufficiently complex to ensure it cannot be easily guessed or misused
- Password shall be a minimum of 8 in characters in length and alphanumeric

- Officers must never share their account and password with anybody, including colleagues, managers, Service Centre, support Officers or family members. Officers are accountable for all activities performed by their accounts

2.4 Reasonable private use

The Association provides information systems for business purposes. Reasonable private use is permitted provided it is infrequent and brief, and does not intrude on your work time, impact on service delivery, incur costs, or create an exposure for the Association to viruses, legal liability, or embarrassment. Officers should also refer to Internet and Email Use Policy for acceptable use of Internet and email services specifically.

2.5 What access or use is not acceptable?

It is prohibited to create, send, access or store information that: ƒ Could damage the reputation of the Association

- Involves or could lead to unlawful victimisation, discrimination, harassment, or vilification
- Is sexually suggestive, offensive, obscene, threatening, abusive or defamatory
- Is used for operating a private business unrelated to the Association
- Is deliberately misleading or deceptive
- Is encrypted without the approval of your manager and does not comply with the Association's encryption standard
- Violates any State or Federal law
- Infringes copyright or other intellectual property rights
- Impersonates another user, their email account, or any other service
- May hinder productivity (such as forwarding chain emails)
- May damage or impair information technology assets (e.g. sending a virus or downloading music or video, use of chat rooms)
- Is for non-business purposes (such as games, music, personal pictures, and videos) other than what is permissible under reasonable private use
- Could potentially destabilise Association systems.

Accessing video or radio broadcasts over the network must be restricted to business use only because of its negative impact on network resources. The Business Manager must approve all requests of this nature.

2.6 Remote Access

Remote access includes all forms of access to the Association network using SSL VPN, or remote wireless and is limited to use by the Association's authorised Officers, authorised organisations and contractors.

Officers with remote access privileges must:

- Protect their remote access account and password from disclosure

- Remain constantly aware that connections between the remote location and the Association are literal extensions of the Association network, therefore provide a potential path to the Association sensitive information
- Beware that all business electronic communication activities become the Association property
- Understand that they have the responsibility for the consequences should remote access be misused
- Ensure there is no other connections existing to any other network at the same time while being remotely connected to Association network
- Comply with the information classification standard while working on protected or highly protected information remotely
- Immediately notify the Service Centre if you suspect any theft or misuse of their remote access account

Wireless connection to the Association network must only use properly secured Wireless Access Points that have been approved by the Information Security and Risk Manager.

2.7 Security Tools

The use of security tools on the Association network is only to be undertaken by approved Association Officers under direction of the Information Security and Risk Manager. Written approval is required from the Information Security and Risk Manager before using a password cracking, scanning, data capturing or other security assessment tool on the Association network.

2.8 Device Connectivity and Configuration

Approval must be sought from the Business Manager before:

- Relocating, connecting, installing, configuring, upgrading, or decommissioning any information technology devices

Approval must be sought from the Information Security and Risk Manager before:

- Disabling or reconfiguring anti-virus software installed on Association equipment
- Connecting any equipment that does not comply with the Association Information
- Security Policy, including privately owned portable computing devices
- Connecting a modem to the Association network

2.9 Information Classification

Progressively all documents will be classified using the Data Classification Scheme and Handling Requirements. The information owners are responsible for determining information classification of their information.

Document owners must ensure compliance with the Data Classification Scheme and Handling Requirements if copying, storing, disposing, or transmitting information. For more information refer to the Data Classification Scheme and Handling Requirements page on the Association's Intranet.

2.10 Securing information

All Officers who are in possession of permanent files and sensitive hard-copy documents must ensure that reasonable steps are taken to protect these from unauthorised access. Simple techniques include keeping your desk clear and using secure storage cabinets where available. The Records Management Policy provides guidance on secure storage of information and must be complied with.

To prevent someone gaining unauthorised access to information or information systems, Officers must activate an approved password-protected screensaver (by pressing Ctl-Alt-Del buttons then select “lock workstation”) or log-out of the Association system or network when leaving the system unattended. Before starting the screensaver, save any files, or close any systems in use to protect it from unauthorised access or corruption. Where voicemail is used, access to the mailbox must be protected by use of a suitable password.

Officers must be cautious when opening files received on external hard drives, floppy disks, CD’s, memory sticks, or by e-mail. Any instance of virus infection must be reported to the Service Desk.

2.11 Intellectual Property and Licensing

Electronic communications, documents and computer software is easily copied which poses a serious risk of infringing of intellectual property. Public domain software that is marked as “free” or “public use” may be for personal use but not for corporate use. When downloading or using free or public use software from the Internet always be aware of license conditions and obtain approval from your manager, as the use of this software may violate copyright or licensing requirements.

Officers must not:

- Copy software, which is licensed to the Association, unless authorised under the license arrangements
- Download and/or install free or non-Association licensed software on any Association equipment

2.12 Officers absences

When a person is absent or on leave, other Officers in the office must not use their account. If there is a need to access another person’s business files while they are away, that Officer should provide “proxy” access to appropriate Officers.

2.13 Protecting information and equipment

Officers must take reasonable steps to ensure that information remains appropriately protected and equipment is physically secured. This especially applies when using portable equipment (such as laptop computers, mobile telephones, pagers, and personal digital assistants (PDA’s)) at non-Association locations.

Association equipment that has been lost or stolen must be reported to Information Security and Risk Manager or Secretary.

2.14 Private and Personal Information

Private and personal information of individuals may only be captured and used in accordance with Privacy and Personal Information Protection Act NSW 1998. Further information can be referenced at: Privacy and Personal Information Protection Act NSW 1998 on the Association Intranet under Policies and Procedures, Legal Matters, Privacy and Personal Information.

2.15 Records Management

All electronic documents and messages (such as email) that relate to the official business of the Association are subject to the same statutory requirements as paper documents. Users must comply with the Association Records Management Policy and procedures when using information technology (such as email and the Internet) for business communications.

2.16 Reporting security breaches

All suspected information security breaches must be reported to your Business Unit Manager, and Information Security and Risk Manager, ServiceFirst IT.

2.17 Access to personal files and removal of unacceptable material

The Association may, without notice or Officers approval, investigate, replicate and/or remove any illegal or unacceptable material from its sites and computing resources. All users should be aware that their use of Association resources, especially for personal purposes is conditional on this right of access by Association management as part of investigations. Using Association resources constitutes consent to its management right of access.

2.18 Monitoring

System privilege and usage may be monitored and reviewed for the effective management of Association resources and under circumstances where it is suspected that the user privileges are being used for illegal, fraudulent, or inappropriate purposes.

All information stored or transmitted on the Association networks or systems may be monitored. Use of Association Information Systems constitutes consent to monitoring of the systems owned by the Association. This is further iterated by the user login warning message.

2.19 Policy Enforcement

Departure from this policy, depending on severity and nature, may result in taking appropriate actions by the Association. This details actions the President may take in the event of a ‘charge’ of misconduct, which include but are not limited to reprimand, loss of access privileges, termination of employment or contract, recovery of costs and/or legal action. Information may be reported to or provided to law enforcement bodies.

3 Related Policies & Documents

- Code of Conduct
- Privacy Policy

- Social Media Policy
- Social Media Guidelines
- Anti-Discrimination, Harassment and Bullying Policy

4 Document Control

4.1 Document Approval

Name & Position	Signature	Date
Greg Wapling, President		13/08/2016
Carol Hadfield, Secretary		13/08/2016

4.2 Document Version Control

Version	Status	Date	Prepared By	Comments
0.9	DRAFT	10/09/2016	Greg Wapling	
1.0	APPROVED	13/08/2016	Greg Wapling	

4.3 Review Date

This policy will be reviewed annually.

It may be reviewed earlier in response to post-implementation feedback from members.