

IT Policies and Procedures Manual

PSAB Australia Pty Ltd



(02)6198 3388



enquiries@psab.net.au



19 Wormald Street, Symonston, ACT 2609
PSAB IT Poli & Proce Ver 1.0 Dated 1-Nov-2020

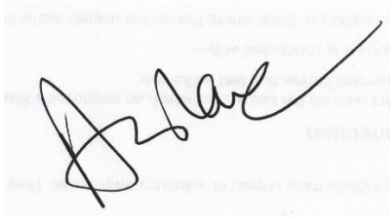
1.0 Introduction

The PSAB Australia Pty Ltd (PSAB) IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business which must be followed by all staff. It also provides guidelines PSAB will use to administer these policies, with the correct procedure to follow.

PSAB will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.
In the event that the CEO is unavailable, [contact the Owner and Public Officer, Rao Ayyalasomayajula]



Kameswara Rao Ayyalasomayajula
Owner, Public Officer

22-Sep-2022



2.0 THP001 - Technology Hardware Purchasing Policy

2.1 Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money and where applicable integrates with other technology for the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

2.2 Procedures

2.2.1 Purchasing desktop computer systems

The desktop computer systems purchased must be compatible with MacOS or Windows operating system and integrate with existing hardware (desktop as a service).

PSAB acquires desktop computer hardware such as Apple based machines and Windows based machines through the finance section of PSAB.

2.2.2 Purchasing portable computer systems

The purchase of portable computer systems includes iPads, MacBook's, and Laptops.

Portable computer systems purchased must be compatible with MacOS or Windows operating systems and integrate with existing hardware (desktop as a service)

PSAB acquires portable computer systems such as Apple based machines and Windows based machines through the finance section of PSAB.

2.2.3 Purchasing Server Systems

PSAB utilises Microsoft Teams services for server systems.

Server systems purchased must be compatible with all other computer hardware in the business.

Any change from the above requirements must be authorised by the CEO.

All purchases for server systems must be in line with the purchasing policy in the Financial policies and procedures manual.

2.2.4 Purchasing computer peripherals

Computer system peripherals include printers, scanners, external hard drives etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.



Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorised by CEO.

Any change from the above requirements must be authorised by CEO.

All purchases for computer peripherals must be in line with the purchasing policy in the financial policies and procedures manual.

2.2.5 Purchasing mobile telephones

The purchase of a mobile phone must be through the Finance section.

The mobile phone must be compatible with the business's current hardware and software systems.

The purchase of a mobile phone must be approved CEO prior to purchase.

Any change from the above requirements must be authorised by CEO.

All purchases of all mobile phones must be supported by the warranty and/or guarantee provided by the manufacturer.

All purchases for mobile phones must be in line with the purchasing policy in the financial policies and procedures manual.



3.0 GS001 - Policy for Getting Software

3.1 Purpose of the Policy

This policy provides guidelines for the purchase of software for the business to ensure that all software used by the business is appropriate, value for money and where applicable integrates with other technology for the business.

3.2 Procedures

3.2.1 Request for Software

All software, including Microsoft Office Suite, Signal, etc., must be approved by CEO prior to the use or download of such software.

3.2.2 Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by CEO.

All purchased software must be purchased from reputable software sellers.

All purchases of software must be supported by warranty and/or guarantee provided by software sellers and be compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by CEO.

All purchases for software must be in line with the purchasing policy in the financial policies and procedures manual.

3.2.3 Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from CEO must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the business's hardware and software systems.

Any change from the above requirements must be authorised by CEO.



4.0 UOS001 - Policy for Use of Software

4.1 Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the business to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

4.2 Procedures

4.2.1 Software Licensing

All computer software copyrights, and terms of all software licences will be followed by all employees of the business.

Where licensing states limited usage (i.e., number of computers or users etc.), then it is the responsibility of CEO to ensure these terms are followed.

CEO is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

4.2.2 Software Installation

All software must be appropriately registered with the supplier where this is a requirement.

PSAB is to be the registered owner of all software.

Only software obtained in accordance with the getting software policy is to be installed on the business's computers.

All software installation is to be carried out by System Administrator.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

4.2.3 Software Usage

Only software purchased in accordance with the getting software policy is to be used within the business.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of Project Coordinator.

Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.



Unless express approval from CEO is obtained, software cannot be taken home and loaded on a employees' home computer

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation CEO is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the business and must be recorded on the software register by System Administrator.

Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to CEO for reprimand action. The illegal duplication of software or other copyrighted works is not condoned within this business and CEO is authorised to undertake disciplinary action where such event occurs.

4.2.4 Breach of Policy

Where there is a breach of this policy by an employee, that employee will be referred to CEO for as reprimand action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify CEO immediately. In the event that the breach is not reported, and it is determined that an employee failed to report the breach, then that employee will be referred to CEO for further consultation.



5.0 BOD001 - Bring Your Own Device Policy

At PSAB we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to PSAB's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

5.1 Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets, and desktop computers for business purposes. All staff who use or access PSAB's technology equipment and/or services are bound by the conditions of this Policy.

5.2 Procedures

5.2.1 Current mobile devices approved for business use

The following personally owned mobile devices are approved to be used for business purposes:

- Android Phones and iPhones.
- Laptops

5.2.2 Registration of personal mobile devices for business use

Employees when using personal devices for business use will register the device with Systems Administrator.

Systems Administrator will record the device and all applications used by the device. Personal mobile devices can only be used for the following business purposes:

- Testing mobile applications.
- Making and receiving phone calls.
- Checking emails.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device.
- Not to use the registered mobile device as the sole repository for PSAB's information. All business information stored on mobile devices should be backed up



- To make every reasonable effort to ensure that PSAB's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected
- To maintain the device with current operating software, current security software etc.
- Not to share the device with other individuals to protect the business data access through the device
- To abide by PSAB's internet policy for appropriate use and access of internet sites etc.
- To notify PSAB immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to PSAB's equipment.

All employees who have a registered personal mobile device for business use acknowledge that the business:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Has first right to buy the device where the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for business use at any time.

5.2.3 Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):



- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g., in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

5.2.4 Exemptions

This policy is mandatory unless CEO grants an exemption. Any requests for exemptions from any of these directives, should be referred to the CEO.

5.2.5 Breach of this policy

Any breach of this policy will be referred to CEO who will review the breach and determine adequate consequences, which can include confiscation of the device and or termination of employment.

5.2.6 Indemnity

PSAB bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify PSAB against any and all damages, costs and expenses suffered by PSAB arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by PSAB.



6.0 ITS001 - Information Technology Security Policy

6.1 Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

6.2 Procedures

6.2.1 Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through secure doors with deadlocks, keypads, and alarm systems.

It will be the responsibility of Security Officer to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify Security Officer immediately.

All security and safety of all portable technology such as laptop, notepads, iPad, mobile phones etc. will be the responsibility of the employee who has been issued with the laptop, notepads, iPads, mobile phones etc. Each employee is required to use locks, passwords, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, CEO will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

All laptop, notepads, iPads, mobile phones, etc. when kept at the office desk is to be secured in a locked draw or class C cabinet with key lock or keypad lock combination provided by Security Officer.

6.2.2 Information Security

All sensitive, valuable, or critical business data is to be backed-up.

It is the responsibility of Security Officer to ensure that data back-ups are conducted daily, and the backed-up data is kept in Microsoft Teams.

All technology that has internet access must have anti-virus software installed. It is the responsibility of System Administrator to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be subject to termination.

6.2.3 Technology Access

Every employee will be issued with a unique identification code to access the business technology and will be required to set a password for access.



Each password is to be at least 8 characters long, with at least 1 number, 1 symbol and 1 capital letter, and is not to be shared with any employee within the business. System Administrator is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out' after 3 attempts, then System Administrator is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

The following table provides the authorisation of access:

Technology – Hardware/ Software	Persons authorised for access
Signal	All PSAB staff.
Microsoft Office 365 Suite	All PSAB staff.
Jira	All PSAB staff.
Harvest	All PSAB staff.
Adobe	All PSAB staff.

Employees are only authorised to use business computers for personal use outside of business operating hours.

For internet and social media usage, refer to the Human Resources Manual. It is the responsibility of IT Manager to keep all procedures for this policy up to date.



7.0 ITA001 - Information Technology Administration Policy

7.1 Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the business.

7.2 Procedures

All software installed and the licence information must be registered on the Microsoft Teams. It is the responsibility of CEO to ensure that this registered is maintained. The register must record the following information:

- What software is installed on every machine
- What licence agreements are in place for each software package
- Renewal dates if applicable.

IT Manager is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by CEO.

IT Manager is responsible for maintaining adequate technology spare parts and other requirements including toners, printing paper etc.

A technology audit is to be conducted annually by IT Manager to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to Systems Administrator.



8.0 WP001 - Website Policy

8.1 Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website.

8.2 Procedures

8.2.1 Website Register

The website register must record the following details:

- List of domain names registered to the business
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

{insert any other records to be kept in relation to your business website here}.

The keeping the register up to date will be the responsibility Website Developer.

Website Developer will be responsible for any renewal of items listed in the register.

8.2.2 Website Content

All content on the business website is to be accurate, appropriate, and current. This will be the responsibility of Website Content Writer.

All content on the website must follow a business or content plan.

The content of the website is to be reviewed monthly.

The following persons are authorised to make changes to the business website:

Managing Director

Website Developer

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the business.

All data collected from the website is to adhere to the Privacy Act



9.0 ET001 - Electronic Transactions Policy

9.1 Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the business.

The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

9.2 Procedures

9.2.1 Electronic Funds Transfer (EFT)

It is the policy of PSAB that all payments and receipts should be made by EFT where appropriate.

All EFT payments and receipts must adhere to all finance policies in the Financial policies and procedures manual.

All EFT arrangements, including receipts and payments must be submitted to Finance section.

EFT payments must have the appropriate authorisation for payment in line with the financial transactions policy in the Financial policies and procedures manual.

EFT payments must be appropriately recorded in line with finance policy in the Financial policies and procedures manual.

EFT payments once authorised, will be entered into the account transfer by CEO.

EFT payments can only be released for payment once pending payments have been authorised by CEO.

For good control over EFT payments, ensure that the persons authorising the payments and making the payment are not the same person.

All EFT receipts must be reconciled to customer records once a month.

Where EFT receipt cannot be allocated to customer account, it is responsibility of CEO to investigate. In the event that the customer account cannot be identified within one month the receipted funds must be allocated to suspense account or returned to source etc. CEO must authorise this transaction.

It is the responsibility of CEO to annually review EFT authorisations for initial entry, alterations, or deletion of EFT records, including supplier payment records and customer receipt records.

9.2.2 Electronic Purchases

All electronic purchases by any authorised employee must adhere to the purchasing policy in the Financial policies and procedures manual.



Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

All electronic purchases must be undertaken using business credit cards only and therefore adhere to the business credit card policy in the Financial policies and procedures manual.



10.0 ITSA001 - IT Service Agreements Policy

10.1 Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the business.

10.2 Procedures

The following IT service agreements can be entered into on behalf of the business:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of business software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

All IT service agreements must be reviewed by PSAB's lawyer before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by CEO.

All IT service agreements, obligations and renewals must be recorded and saved in Microsoft Teams

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by Systems Administrator.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, PSAB's lawyer should review before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by CEO.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to CEO who will be responsible for the settlement of such dispute.



11.0 EMIT001 - Emergency Management of Information Technology

11.1 Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the business.

11.2 Procedures

11.2.1 IT Hardware Failure

Where there is failure of any of the business's hardware, this must be referred to System Administrator immediately.

It is the responsibility of System Administrator to ensure all files are backed up in the event of IT hardware failure.

It is the responsibility of IT Manager to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to business operations.

11.2.2 Virus or other security breach

In the event that the business's information technology is compromised by software virus or hacking such breaches are to be reported to Cyber Security team immediately.

CEO is responsible for ensuring that any security breach is dealt with within 24 hours to minimise disruption to business operations.

Website Disruption

In the event that business website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- Website Developer and Managing Director must be notified immediately
- Post a notification to viewers about website being down for maintenance.

