TOSHIBA

PRIVACY POLICY

(POL-ADMIN-3.20)

Note: This is a TIC AS/NZS ISO 9001:-Quality Management System controlled document. The only controlled copy is maintained electronically in TIC's document management systems. Any printed copy of this document is an uncontrolled copy and should be used for reference only.

DOCUMENT REVISION HISTORY

Rev No.	Revision Date	Reason for Change	Written by	Checked by	Approved by
0	June 2018	Initial writing	TS	RR	
1	28 Nov 2022	Review	TS	RR	MS

Review Committee

Name	Division / Department
Remy Reinker	Finance
Ben Dugan	HR Manager
Susie Vang	Payroll
Tricia Silverosa	Administration
Paul Sistrom	Legal Dept

TABLE OF CONTENTS

Page

1.0 PURPOSE

Privacy in Australia is governed by the Commonwealth *Privacy Act 1988* (the Privacy Act). It applies to most private sector organisations, as well as Commonwealth and territory government agencies.

The Privacy Act requires compliance with 13 Australian Privacy Principles (IPPs) that regulate how applicable organisations and agencies handle personal information.

TIC collects, holds, uses and discloses personal information so that it can establish, manage and administer the sale and purchase of goods and services provided by TIC to its customers and to enable TIC to comply with relevant legal and regulatory obligations.

TIC respects the privacy of the people its deals with, including its officers and employees, and endeavours to uphold high standards of privacy practice and security.

TIC is committed to protecting the privacy of the data that it collects, including from its officers, employees, suppliers, customers, consultants and contractors.

This policy explains how TIC collects, uses and discloses information.

2.0 SCOPE

This policy applies to all personal information collected and maintained by TIC from persons including officers, employees, contractors, consultants, shareholders, suppliers and also customer information collected by TIC.

This policy does not apply to:

- publicly available information ie on TIC's website, social media sites; and
- information required to be accessed via government legislation, regulations etc.

3.0 REVIEW & APPROVAL

The document may be reviewed due to:

- compliance issues resulting from legislation, regulations and company policy and procedures
- audit findings
- feedback from workers and key stakeholders
- organisational change
- other relevant information.

Review of or changes to this procedure require approval of the Managing Director.

Any other matters that may not have been specifically addressed in this policy will be dealt with at the discretion of TIC's Managing Director and/or General Manager – Finance & Administration.

4.0 ABBREVIATIONS

HR	Human Resources
TIC	Toshiba International Corporation Pty Ltd

5.0 DEFINITIONS

Personal Information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) (b) whether the information or opinion is recorded in a material form or not.

Sensitive Information	means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
Related Body Corporate	has the meaning given to that term in the *Corporations Act 2001* (Cth).

6.0 COMPLIANCE

6.1 Noncompliance impact on TIC

Failure to comply with this policy could result in negative outcomes (e.g. inappropriate disclosure of personal information, falsification of records, fraudulent behavior, complaints) and is a non conformity during internal and external audits of TIC's financial management systems.

Breaches of this policy will be investigated as potential breaches of TIC's Standards of Conduct. Any actions taken will be based on outcomes from the investigation.

6.2 Policy enforcement

Failure to comply with this policy may lead to disciplinary action.

6.3 Policy implementation

Implementation of this policy shall take effect from the date of policy approval.

7.0 USE OF PERSONAL INFORMATION

TIC uses personal information for the purpose for which it was provided to TIC, including to:

- process payments
- communicate with the user and authorised third parties.

TIC does not sell personal information to other organisations for marketing purposes.

8.0 TYPES OF INFORMATION COLLECTED

TIC will collect personal information from its employees, officers and stakeholders for its business operations such as payroll, workplace health and safety, human resources etc.

This is necessary for TIC to fulfil its legal obligations such as those relating to taxation, safety and financial concerns eg bribery, fraudulent behaviour.

Some examples of personal information collected for these purposes are:

- the terms and conditions of employment of an employee or contractor including wages, salaries
- personal and emergency contact details
- the employee's performance or conduct
- the engagement, training, disciplining or resignation or termination of the employee
- the employee's taxation, banking or superannuation affairs
- credit applications from customers
- credit reporting bodies.

The fact that a record does not mention a person's name does not preclude it from being personal information.

Personal information may also be collected by TIC in the course of its business dealings with actual or potential customers and suppliers. This information may include the names and contact details of principals, officers or employees of actual or potential customers and suppliers.

Sensitive information (as defined above) is a subset of personal information and is subject to higher levels of protection under the Privacy Act.

TIC does not collect sensitive information unless required by law or where there is a demonstrated business need and consent is given to do so. This type of information may be required in circumstances including assessing a workers compensations claim, harassment/discrimination report, or fraudulent behaviour.

A record can be considered to be "personal information" by checking whether the particular record contains information which could in some way enable identification of an individual.

TIC recognises that not all information it has about an employee should be considered to be an employee record. This is most relevant when the information held is not related to the employment relationship e.g. some emails an employee receives from another party.

Generally, information that is anonymous or depersonalised will not be viewed as personal information.

9.0 HOW INFORMATION IS COLLECTED

Personal information can be collected through

- face to face meetings
- information given directly to TIC via completed employment forms, documentation, telephone, email, internet
- other methods.

10.0 ACCURATE PERSONAL INFORMATION

TIC will take reasonable steps to ensure that all personal information held is as accurate as possible. Individuals are able to contact TIC and ask for correction of personal information relating to them, if the information is inaccurate or incomplete.

11.0 ACCESSING PERSONAL INFORMATION

Generally (but subject to Australian law), TIC will give an individual full access to their personal information within a reasonable time and in the manner requested by them.

However, there may be some circumstances when this is not possible, including where:

- TIC no longer hold or use the information
- providing access would have an unreasonable impact on the privacy of others
- the request is frivolous or vexatious
- providing access would be unlawful.

If access is not provided, then TIC will inform the individual of the reason for the denial.

12.0 PERSONAL INFORMATION STORAGE

TIC keeps personal information in physical and electronic records at TIC's premises and/or the premises of its service providers which may include processing or storage on non-TIC servers.

TIC will take steps to protect the security and integrity of personal information, including protecting digitally stored data.

13.0 PERSONAL INFORMATION SECURITY

Access to personal information is restricted to employees, officers and stakeholders (other than the individual to whom the personal information relates) who need it to provide a service (e.g. payroll).

TIC will protect personal information from misuse, loss, unauthorized access, modification or improper disclosure through physical, technical and administrative safeguards. This may be in a combination of secure computer storage facilities, paper based files and other formats.

When there is no requirement to keep the personal information, it will be deleted, destroyed or de-identified.

14.1 System security

TIC takes reasonable steps to prevent unauthorized access to its online and computerised systems by using measures such as firewalls, data encryption, virus detection methods and password restrictions.

IT Dept will update and test security technology on an ongoing basis.

14.2 Physical security

At TIC business premises, only authorised personnel have access to dedicated and/or restricted areas eg HR, payroll, server rooms by using electronic access methods that control and monitor this access.

14.3 Employee training

Training is provided to TIC employees about the importance of confidentiality and maintaining privacy and security of confidential and/or personal information.

14.4 Third parties

TIC takes reasonable steps to ensure that third parties who store or assist TIC to store personal information adopt appropriate security measures.

14.0 DISCLOSING PERSONAL INFORMATION

Subject in all cases to local law and regulations, TIC may share personal information with its Related Bodies Corporate and may disclose personal information outside of TIC:

- as required by law, regulations or regulator
- to TIC service providers such insurance, website maintenance, auditing, accounting.

TIC may also disclose personal information in connection with the management of any parts of TIC's business or assets. This may include disclosure to law enforcement agencies, the Australian Taxation Office, national government and regulatory authorities.

TIC will disclose personal information when there is a reasonable basis to:

- protect the safety, privacy and security of other users
- protect against fraud or for risk management purposes
- protect, enforce or defend the legal rights of TIC
- comply with the law or legal processes in any country
- respond to requests from public and government authorities.

15.0 COMPLAINTS

If TIC has breached the Privacy Act or other applicable privacy laws, a person can contact TIC to make a complaint.

This complaint will be handled in accordance with TIC's company policies and guidelines.

If the complaint is not resolved, the user can then lodge a complaint with the Australian Information Commissioner.

16.0 VARIATION TO THIS POLICY

Variations to this policy will only take place under the specific direction of the Managing Director and/or General Manager – Finance and Administration Division.

End of policy.