TOUCH PROJECTS

Information Security Management Policy

Information security is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities.

This Information Security Management Policy applies to Touch Projects Limited, it's preceding and owning entities, and any related legal entities or trusts.

PART 1. Background Information

Information security is the protection of information and supporting systems from a wide range of threats in order to ensure business continuity, minimise operational risk, and maximise return on investments and operational opportunities.

The policy is aligned with the Australian and New Zealand Information Security Industry Standard - Information technology - Code of practice for information security management.

PART 2. Policy Purpose

This policy outlines how Touch Projects will manage and mitigate security risks to safeguard the confidentiality, integrity and availability of information and communication technology assets and environment. Data, Information and the underlying technology systems are essential assets to Touch Projects and require to be suitably protected.

Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that specific security objectives are met.

Touch Projects is committed to providing a secure, yet open information environment that protects the integrity and confidentiality of information without compromising access and availability.

The purpose of the Information Security Management policy is to:

i. Set out the security requirements that Touch Projects must meet to manage the Confidentiality, Integrity, Availability and Privacy of Touch Projects owned data and information, and

ii. Ensure that Touch Projects can meet its obligations with applicable laws, regulations, and standards.

Information Security Management Policy

PART 3. Policy Application

This policy applies to all information that is electronically generated, received, stored, printed, or keyed, and to the IT applications and systems that create, use, manage and store information and data. The policy covers the following areas:

i. Access Control – To limit access to information and information processing facilities in support of business requirements. Access to Touch Projects' information and systems must be:
   - Attributable to a uniquely identifiable individual who is responsible for actions performed with their system account.
   - Based on the requirements of the individual's role, and
   - Managed by passwords, routinely revalidated, and removed if no longer required.

ii. Digital Messaging – To establish and maintain the protocol for using Digital Messaging in all its forms, including the security aspects of information transfer with any external entities.

iii. Communications and Operation Management – To ensure the protection of information and the secure operations of networks.

iv. Physical and Environmental Security – To prevent unauthorised physical access, damage and interference to Touch Projects' information.

v. System Acquisition, Development and Maintenance – To ensure that information security is an integral part of information systems across the entire lifecycle.

vi. Supplier Relationships – Touch Projects will implement security controls and processes to manage supplier access to information assets. Suppliers and vendors will be given access privileges only at the level required to deliver contracted services.

vii. Information Security Incident Management – To ensure a consistent and effective approach to the management of information security incidents, including security events and vulnerabilities.

viii. Compliance Management – To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security.

ix. The provisions of this policy apply to all personnel, (including temporary agents and staff engaged under contract). This policy includes, but is not limited to:
   a. Touch Projects information in any form, including print, electronic, audio, backup and archived data. This includes computer systems, websites, email servers, software applications, databases, and operating systems.
   b. Physical premises occupied by the personnel and equipment.
   c. Processes, policies and procedures; and
   d. Transmission of communications and related pathways.

PART 4. Policy Principals

This Information Security Policy defines the principles for establishing effective security measures to ensure the confidentiality, integrity, availability and privacy of Touch Projects' information.

The Policy also covers the continued availability of information and the Information Environment to support business activities, including the implementation of appropriate controls to protect information from intentional or accidental disclosure, manipulation, modification, removal or copying.

The following principles outline the minimum standards that guide the Information Security processes and procedures and must be adhered to by all personnel.

4.1 Touch Projects Responsibilities

Touch Projects is responsible for safeguarding the

Information Security Management Policy

Information Environment and Information Resources against security threats. Touch Projects discharges its responsibilities through the following section of this Policy:

i. Defining roles and responsibilities and establishing clear lines of accountability.

ii. Protecting Touch Projects' information assets against internal and external threats. (e.g. security breach, loss of data)

iii. Ensuring that the Touch Projects complies with applicable laws, regulations, and standards.

iv. Identifying and treating security risks to the Touch Projects information environment through appropriate physical, technical and administrative channels, and

v. Developing best practices for effective Information Security across Touch Projects.

4.2 User Responsibilities

i. Users must abide by all relevant laws and all Touch Projects policies.

ii. Users are expected to take responsibility for developing an adequate level of information security awareness, education, and training to ensure appropriate use of the information environment.

iii. Users may only access information needed to perform their authorised duties.

iv. Users are expected to determine and understand the classification of the information to which access has been granted through training, other resources or by consultation with the relevant manager.

v. Users must protect the confidentiality, integrity and availability of Touch Projects' information as appropriate for the information classification level.

vi. Users may not in any way divulge, copy, release, alter or destroy any information, except as authorised by the relevant manager.

vii. Users must safeguard any physical key, ID card or computer/network account that enables access Touch Projects information. This includes maintaining appropriate password creation and protection measures as set out in the password composition guidelines.

viii. Any activities considered likely to compromise sensitive information must be reported to the relevant manager or IT support services, and

ix. Users are obliged to protect sensitive information even after separation from Touch Projects.

4.3 Managers

In addition to complying with the requirements listed above for all staff and contractors, managers must:

i. Ensure that the procedures support the objectives of confidentiality, integrity and availability and that those procedures are followed.

ii. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic, and

iii. Ensure that each staff member understands their information security related responsibilities.

4.4 System and Technology Managers

In addition to complying with the stated policy requirements defined for all staff, contractors, managers, system and information environment managers are responsible for:

i. Ensuring adequate security for computing and network environments that capture, use or store information.

ii. Ensuring that the requirements for confidentiality, integrity, privacy and availability are being appropriately managed within their respective environments.

iii. Understanding the classification level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.

Information Security Management Policy

iv. Developing, implementing, operating and maintaining a secure information environment that includes:

v. System implementation and configuration.

vi. Procedures & guidelines for administering network and system accounts and access privileges, and

vii. An effective strategy for protecting information against generic threats for the system or service.

PART 5. Risk Assessment

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the operational damage likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls to protect against these risks.

Responsibilities for risk assessment and treatment are clearly defined in the Touch Projects' Risk Management register.

PART 6. Network Access Classification

Touch Projects network access classification is defined under the two broad headings:

- Management, and
- Team

PART 7. Changes

We reserve the right to modify this Policy from time to time. Any updates will be e-signed as per the approvals section on page 4.

We will always ensure that a current version of this policy is available on the Touch Project website.

PART 8. Contact Us

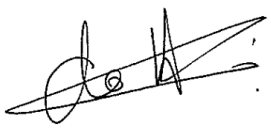
If you have a query or complaint, or would like further information about this Policy, you can contact us by emailing admin@touchprojects.com.au.

We will investigate your queries and complaints as quickly as possible and notify you of the outcome within a reasonable period of time.

PART 9. Document Approval

This document is approved on the date of the last signature below.

Nick Savvas
CEO



John Christou
General Manager

Policy issued on:	3 March 2023	Review Date:	3 March 2024