PRIVACY POLICY

Document Management	
Owner	Tania Armstrong – Privacy Officer
Prepared by:	Tania Armstrong – Privacy Officer
Version:	V2
Date:	7 March 2022
Review Date:	6 March 2023

STATE3 SECURITY AND PRIVACY POLICY

STATEMENT

Thank you for entrusting STATE3 New Zealand Limited (STATE3) with helping your organisation visualise, manage, and improve your technology current state. We appreciate that we are holding private information and that it is a serious responsibility; we want you to know that we understand this and want to let you know how we are handling it.

As our client, we collect information about your organisation in two ways:

1. As part of our business-as-usual activities; and
2. As part of providing your or your employees access to STATE3 Online (SaaS)

We only collect the information you choose to give us, and we process it with your consent, we only require the minimum amount of personal data and do not sell, provide access to any third party – we only use it as outlined by this statement.

Scope

This document is a STATE3 wide policy for New Zealand. It covers our internal approach to security and privacy but also the steps we take on behalf of the clients we work with.

Application

This policy applies to all employees of STATE3 Limited; whether at the STATE3 Limited offices or elsewhere, and refers to all internal resources, technology based or otherwise which they will have access to in helping STATE3 deliver its service to our end clients.

Purpose

STATE3 services - both professional services and access to STATE3 Online, and all internal systems and resources provide a service to our clients to assist them with 'visualising, managing and improving their technology current state'. The purpose of this policy is to define responsibilities within STATE3 for maintaining the security of:

- STATE3 NZ Limited, and
- STATE3 Limited
- Client data relating to their internal operations and contractual information relating to the provision of STATE3 services.

By implementing this policy STATE3 Limited will:

- protect against unauthorised access to, or unauthorised use or sharing of data that could potentially result in harm to the STATE3 Limited or our clients.
- protect against anticipated threats or hazards to the security of STATE3 resources
- comply with legal requirements, STATE3 Limited policies and any agreements binding the STATE3 Limited to implement applicable security safeguards

Definitions

For purposes of this policy, unless otherwise stated, the following definitions shall apply:

Privacy Officer: A STATE3 manager-level employee, responsible for ensuring that STATE3 complies with the Privacy Act 2020[1]. This includes dealing with requests made to the organisation for access to, or correction of, personal information and working with the Privacy Commissioner during the investigation of complaints.

[1] Please refer to https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

Security Officer: A STATE3 the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. This includes internal permissions by employee for whom can work with, have access to classified client and STATE3 data.

Information Asset: Information assets are data, information, knowledge, or expertise in any form. They may include financial, operational, or contractual information;

Information Owner: The information owner is generally the person responsible for the function, process or project that collects, processes **or** creates information.

Information Classification: Client information is classified as part of the STATE3 Online Steering Committee.

Information Security: Assurance that the confidentiality, integrity and availability of information assets are maintained to the appropriate degree.

Confidentiality: The protection of sensitive or private information assets from unauthorised disclosure.

Client User: Any users accessing STATE3 as authorised by a contracted client of STATE3.

STATE3 Employee: This includes anyone working for STATE3 Limited, and includes all staff (whether permanent, temporary or part time), students / interns (whether full time or part time), contractors, subcontractors, consultants, business partners or official visitors or guests of members of the STATE3 Limited.

Security safeguards: are measures undertaken to protect IT resources

Sensitive data: refers to data whose unauthorised disclosure may have serious adverse effect on individuals, clients or on the STATE3 Limited's reputation, resources, or services

Integrity: The accuracy, completeness and validity of information. Integrity also means that an information asset has not been modified without authorisation.

Security Incident: this relates to and includes an attempted or successful unauthorised access, use, disclosure, modification or destruction of information, or interference with STATE3 Online, any systems pertaining to the online solution or internal STATE3 operational systems.

1) Policy Content and Guidelines

a) Information Security Governance

i) The STATE3 Executive shall oversee an information security programme, which shall include information security strategy, principles, policy, objectives, and other relevant components.

ii) The programme shall include means of ensuring that STATE3 stakeholders are involved in changes affecting their service via our STATE3 Online User Forum, or directly via account meetings, workshops or training sessions.

iii) The programme shall include means for ensuring effective communication in support of information security.

iv) Management shall allocate sufficient resources and staff attention to adequately address information security.

2) Roles and Responsibilities

a) STATE3 End Users

i) Information security is every user's responsibility, and it is the end user's obligation to understand their specific responsibilities for information security as it is outlined within their own organisation.
ii) Access to STATE3 is provided on a contracted number of user's basis as outlined within the Contract for Service.
iii) End users are required to abide by the Acceptable Use Policy which is provided as part of the initial contract between STATE3 and client.
iv) End users also access this policy when first accessing STATE3 Online for the first time. Any usage of the service is considered compliance.
v) Any security infringements noticed by the client should be escalated to the Security Officer at STATE3.

3) STATE3 Management

a) Managers are responsible for promoting security as a part of standard operating procedures.
b) Managers are responsible for ensuring the prompt adjustment of appropriate system permissions when changes to a user's role or status occur as requested by the client.

4) STATE3 Information Classification

a) STATE3 Online information is classified as part of the product steering committee, chaired by the Security Officer.
b) The steering committee is responsible for:
   i) determining the value of the data or information;
   ii) classifying the information according to the classification standard;
   iii) deciding who can access the information;
   iv) ensuring that risk assessments for the information assets are performed;
   v) ensuring that appropriate controls are in place.
c) These responsibilities may not be delegated by any member of the steering committee.

Note: The information owner may seek advice and assistance in carrying out these responsibilities.

5) STATE3 Privacy Officer

a) The STATE3 Privacy Officer is responsible for the application of the Privacy Act principles (and impending changes) within STATE3;
   i) work to make sure STATE3 complies with the Privacy Act 2020;
   ii) deal with any complaints from STATE3 clients about possible breaches of privacy;
   iii) deal with requests for access to personal information, or correction of personal information
   iv) act as the agency's liaison with Office of the Privacy Commission;

6) STATE3 Cyber Security Officer

a) The STATE3 Cyber Security Officer is responsible for:
   i) directing and coordinating the STATE3 Limited-wide IT Security Programme determining unit level compliance with this policy;
   ii) providing a focal point for oversight of serious security incidents
   iii) establishing security metrics, tracking the progress of the IT Security Programme and providing a **STATE3** Limited-wide IT risk profile; and
   iv) ensuring availability of appropriate information, education and training.

7) Remedial Actions

This document is a principal-based policy, requiring the following actions to be taken as part of normal communications for business-as-usual changes or maintenance.

a) Proactive Measures

1. STATE3 customers (or potential customers) are welcome to review our policies, ask questions and request changes to our policies.
2. User agreements outline the service level agreements for access to the service.
3. STATE3 will advise users of planned outages via their SaaS access.
4. Release notes is embedded within STATE3 Online in the Version. All details of changes including measures taken to secure the service will be housed
5. STATE3 takes no responsibility for client-users accessing or use the system. All background checks or client-user vetting is the responsibility of the client organisation.
6. STATE3 Online permissions are allocated by the client organisation.

8) Security Breaches

a) In the event of a suspected security breach, we will take the following actions as practicable.

i) Contain and Assess

(1) stopping any unauthorised practices
(2) trying to get the lost information back
(3) disabling the breached system
(4) cancelling or changing computer access codes
(5) trying to fix any weaknesses in your agency's physical or electronic security.
(6) Determine communication pathways (e.g. insurer, internal auditors, risk managers, legal advisors).

ii) **Evaluate the Risks**

(1) Types of personal information involved
(2) The impact of the personal information and understanding of potential harm.
(3) The cause of the breach
(4) The extent of the breach
(5) The potential harm of the breach
(a) identity theft
(b) financial loss
(c) loss of business or employment opportunities
(d) significant humiliation or loss of dignity

iii) Notification and communications pathways.

(1) In the event of a confirmed and impactful breach STATE3 will ensure that any risk or harm to a person will be promptly communicated unless to do so will further impact the person involved.
(2) On a case by case basis the following considerations will assist in determining the appropriate approach to notification.
(a) the risk of harm to people affected
(b) whether there's a risk of identity theft or fraud
(c) whether there's there a risk of physical harm
(d) whether there's a risk of humiliation, loss of dignity, or damage to the person's reputation or relationships.
(e) what affected people can do to avoid or minimise possible harm, e.g. change a password
(f) whether you have any legal or contractual obligations.

iv) Notification approaches

(a) It is expected that any breaches should be communicated in the most efficient way possible (e.g. phone) and followed up by email / letter with further details once known.

v) Communication points

(a) The following key points should be communicated as known at the time.
  (i) information about the incident, including when it happened
  (ii) a description of the compromised personal information
  (iii) what STATE3 is doing to control or reduce harm
  (iv) what STATE3 is doing to help people the breach affects
  (v) what steps people can take to protect themselves
  (vi) contact information for enquiries and complaints
  (vii) offers of support when necessary, e.g. advice on changing passwords
  (viii) whether STATE3 has notified the Office of the Privacy Commissioner
  (ix) contact information for the Privacy Commissioner.

(b) Notifying third parties
  (i) As part of the assessment processes, STATE3 will determine if third parties should be advised. It is our approach that in any situation where personal harm or risk is increased or financial or security of a client is compromised, we will escalate to the most appropriate authorities – Office of the Privacy Commissioner (https://www.privacy.org.nz)

(2) Media Interest

(i) Should the media become alerted to a breach in STATE3 systems or policies, we will work with our PR / Coms team to address the situation when the facts are confirmed.

(3) Prevention of Repeat Breaches

(a) It is important to consider lessons learned and to ensure that all matters are clearly documented with remedial actions taken, an assessment of those actions and preventative considerations included into our services and internal policies. This will be completed at the earliest

(b) The review of the breach will reflect the significance of the breach and the cause (e.g. systemic problem or isolated event), however the following points should be considered:
  (i) security audit of both physical and technical security
  (ii) review of policies and procedures
  (iii) review of employee training practices
  (iv) review of any service delivery partners caught up in the breach.

Document End