BASTION

SECURITY GROUP

BASTION SECURITY GROUP

Privacy Policy

Overview

Policy Statement

Bastion Security Group is committed to providing quality services to you, and this policy sets out our obligations to you in how we manage your personal information. Our business is security, so you know we take your privacy seriously.

Bastion has adopted the Information Privacy Principles under the New Zealand Privacy Act 2020 and the Australian Privacy Principles under the Australian Privacy Act 1988. These principles govern the way Bastion collects, uses, discloses, stores, secures and disposes of your personal information.

Scope

This policy applies to personal information collected or held by Bastion Security Group Limited and its subsidiary Cythera Pty Ltd, in any format, and to personal information handled on Bastion's behalf by its personnel and its suppliers.

It covers personal information about the people Bastion deals with, including customers and their personnel, prospective customers, website visitors, suppliers and their personnel, job applicants, employees and contractors.

Bastion holds personal information in two different capacities, and which one applies changes what Bastion can do with the information and who you should approach about it. The next section explains the difference, and the rest of this policy should be read in that light.

Definitions

Term	Description
Personal information	Information about an identifiable individual, whether true or not, and however recorded. Includes your name, contact details, employment or engagement details and any information that could reasonably identify you, either alone or combined with other information Bastion holds.
Sensitive information	A subset of personal information given heightened protection under privacy law, including information about racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership, sexual orientation, criminal record or health, genetic or biometric information.
Customer engagement material	Information Bastion receives, generates or holds in the course of delivering a service to a customer, including managed service platform data, security monitoring telemetry, forensic images, investigation material, penetration test results and security assessment material. It frequently contains personal information about the customer's own people or its customers.
Privacy breach	Unauthorised access to, disclosure of, or loss of personal information, whether or not it also constitutes an information security incident.
Notifiable privacy breach	A privacy breach that has caused, or is likely to cause, serious harm to one or more individuals, meeting the threshold requiring notification to the Office of the Privacy Commissioner (New Zealand) or the Office of the Australian Information Commissioner, and to affected individuals, under the New Zealand Privacy Act 2020 and the Australian Privacy Act 1988 respectively. Not every privacy breach is a notifiable privacy breach; only a breach meeting this threshold is.

Term	Description
De-identification	Removing or altering information so that an individual can no longer reasonably be identified from what remains, either directly or by combining it with other available information.

The Capacity in Which Bastion Holds Your Personal Information

Bastion is a security services business. Much of the information it handles belongs to its customers rather than to Bastion, and includes personal information about those customers' own employees, contractors and customers. Bastion therefore holds personal information in two distinct capacities.

- **(a) As an organisation in its own right:** this is personal information Bastion collects and holds for its own business purposes, and about which Bastion decides what is collected, why and who it is shared with. It includes information about Bastion's own employees, contractors and job applicants, its customer and supplier contacts, prospective customers, website visitors and enquirers. In this capacity Bastion is an agency under the New Zealand Privacy Act 2020 and an APP entity under the Australian Privacy Act 1988, and this policy's commitments apply to Bastion directly.
- **(b) On a customer's behalf, under an engagement:** this is personal information contained in customer engagement material, which Bastion holds only so that it can deliver the service the customer has engaged it for. The customer decides what is collected, why and who it is shared with; Bastion acts on the customer's instructions and under the terms of the engagement. Under section 11 of the New Zealand Privacy Act 2020, information held by an agency solely as an agent is treated as held by the organisation it acts for. Under Australian privacy law Bastion holds this information under a commercial engagement, with its obligations set by that engagement and by the Australian Privacy Principles. Bastion is not entitled to disclose, correct or delete this information on its own authority, except where the law requires Bastion to disclose it, including a privacy breach notification as described below.

What this means in practice:

- If you want to access, correct or delete personal information that Bastion holds in capacity (a), contact Bastion directly using the details in Privacy Enquiries and Complaints, below.
- If your request concerns personal information Bastion holds in capacity (b), the organisation that engaged Bastion is the right party to approach, because it is the organisation that decides what happens to that information. If you contact Bastion instead, Bastion will refer your request to that organisation within 5 working days of establishing that the information is held in this capacity, tell you that it has done so and tell you who it has been referred to, unless the engagement terms or the law prevent Bastion from disclosing that.
- Bastion records which capacity applies to the information involved in each engagement at the point the engagement is set up, so that this is settled before a request or an incident arrives rather than during one.

Privacy breaches are handled differently from access and correction requests. Where a breach affects personal information Bastion holds in either capacity, Bastion assesses whether the breach is notifiable and decides whether notification is required. Bastion does not leave that decision to the customer. Both Bastion and the customer may carry a notification obligation in their own right, and a notification made by one of them can satisfy both, so the risk that matters is that a required notification is not made at all.

In practice this means:

- Bastion tells the affected customer as soon as it establishes that a breach affects information held under their engagement, and works with them on the assessment.

- Bastion consults the customer before notifying a regulator wherever it is practicable to do so, and takes their view seriously. Where Bastion concludes that notification is required and agreement cannot be reached in time, Bastion notifies the regulator anyway.
- Where affected individuals must be told, the notification is usually made by the organisation that holds the relationship with them, which is normally the customer rather than Bastion. Bastion decides that notification is required, agrees who makes it and confirms that it has been made. Where the customer cannot or will not notify, Bastion notifies the individuals itself where it is able to.
- Bastion does not treat an incident as closed until any required notification has been made.

The Personal Information Bastion Collects and Holds

The personal information Bastion collects depends on your relationship with it. It generally falls into four groups:

- **Identity and contact information:** your name, email and postal addresses and contact numbers.
- **Corporate information:** your employer's details, its business number, its office addresses and its financial standing where Bastion is assessing it as a customer or supplier.
- **Technical information:** online identifiers, account names, access records and, for the Bastion website, the information described under Cookies and Website Analytics, below.
- **Business contact and prospect information:** your name, job title, employer, work email address, work phone number and professional profile, held so that Bastion can identify organisations that may need its services and reach the right person at them. Where this comes from is described under How Bastion Collects Personal Information, below.

Where Bastion is delivering a security service, customer engagement material may contain a much wider range of personal information about the customer's own people. That information is held in capacity (b) described above, and the customer determines what it contains.

How Bastion Collects Personal Information

Bastion collects personal information in a number of ways, including directly from you in meetings, interviews and correspondence, by telephone and email, through the Bastion and Cythera websites, from your organisation's own systems where Bastion has been engaged to work on them, from publicly available sources and media and from third parties such as recruiters and referrers.

Bastion also obtains business contact information from public professional and company sources and from third-party business data and sales intelligence providers. What is obtained this way is work-related rather than personal or domestic: your name, your job title, your employer, your work email address, your work phone number and your professional profile. Bastion uses it to identify organisations that may need its services and to reach the right person at those organisations.

Where it is reasonable and practicable to do so, Bastion collects your personal information directly from you. Where Bastion is given your personal information by a third party, it takes reasonable steps to make sure you are made aware of that, unless an exception under privacy law applies.

Where your information reached Bastion from a business data provider or a public source rather than from you, this policy is one of those steps, and Bastion will tell you which provider or source your details came from if you ask. You can ask Bastion to stop contacting you, and to delete what it holds about you, at any time using the details under Privacy Enquiries and Complaints, below. A request to stop contacting you is actioned whether or not the underlying record is also deleted, and where Bastion keeps a record solely so that your details are not acquired again from the same provider, it holds that record for that purpose alone.

When Bastion collects personal information from you it will, where appropriate and practicable, explain why it is being collected and how it is intended to be used.

Sensitive Information

It is Bastion's policy not to collect or store sensitive information. In the rare cases where Bastion does hold sensitive information, for example where a customer engagement or a legally required background check makes it unavoidable, Bastion uses it only:

- for the primary purpose for which it was obtained;
- for a secondary purpose directly related to that primary purpose;
- with your consent; or
- where required or authorised by law.

Sensitive information Bastion does hold is classified at the highest level under Bastion's Data Management Policy and handled under that policy's strictest controls.

How Bastion Uses Personal Information

Bastion collects and uses your personal information so that it can deliver the services you or your organisation have asked for. Bastion may also use it to contact you about new offerings and to assess how well it is delivering its existing services to you.

Bastion may use your personal information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect that use, and where required or authorised by law.

Bastion may also contact you from time to time on behalf of its business partners about an offering that may be of interest to you. Where it does, Bastion contacts you itself rather than passing your details to that partner for the purpose of marketing to you.

Bastion may share your personal information with trusted partners so that they can carry out performance or statistical analysis on Bastion's behalf, send email or postal mail to you and arrange deliveries. Those partners may use your personal information only to provide that service to Bastion and are required to keep it confidential.

Where Bastion contacts you by electronic message or by telephone, it does so in accordance with the laws that apply to that contact as well as with privacy law, including the Spam Act 2003 (Cth), the Unsolicited Electronic Messages Act 2007 (NZ) and the Do Not Call Register Act 2006 (Cth).

Every direct marketing message Bastion sends includes a simple way to opt out. You may also unsubscribe from Bastion's mailing and marketing lists at any time by contacting Bastion in writing. Once Bastion receives your request, it will stop using your personal information for direct marketing. You may also ask Bastion where it obtained your contact details, and Bastion will tell you unless it is unreasonable or impracticable to do so.

Disclosure and Third-Party Sharing

Bastion does not sell, rent or lease your personal information to third parties.

Your personal information may be shared with a third party in the following circumstances:

- where you have given your explicit consent;
- where Bastion holds the information in capacity (b) above, with the organisation that engaged Bastion, in line with the agreed terms of that engagement;
- with Bastion's suppliers, subject to the agreed terms of service and on a basis of processing consistent with this policy;
- with Bastion's business partners, for the direct marketing and fulfilment purposes described under How Bastion Uses Personal Information, above;
- with Bastion's affiliates and partners, subject to non-disclosure agreements and for a legitimate purpose consistent with this policy; and
- where required or authorised by law, for example to a government agency, regulator or law enforcement agency acting for a lawful purpose.

Bastion uses third-party suppliers located both in Australia and New Zealand and overseas. These services may include software that accesses personal information in its ongoing operation and during the provision of support.

The categories of supplier that may access personal information are:

- cloud infrastructure and productivity platforms;
- finance and customer relationship management systems;
- business contact data and sales intelligence providers;
- support ticketing and internal knowledge base tools;
- messaging and email delivery services;
- website analytics;
- managed security and compliance vendors; and
- marketing and customer events providers.

A current list of the suppliers in these categories is available on request, using the details under Privacy Enquiries and Complaints, below.

Before Bastion shares personal information with a supplier, that supplier is assessed and contractually bound under Bastion's Third-Party Management Policy. Suppliers are prohibited from using your personal information for anything other than providing their service to Bastion, and are required to maintain its confidentiality.

Overseas Disclosure

Bastion operates in New Zealand and Australia. Some of the suppliers and systems it uses store or process personal information overseas, most commonly in the United States. The countries a supplier operates from are included in the supplier list available on request under Disclosure and Third-Party Sharing, above.

Before your personal information is disclosed to an overseas recipient, Bastion takes reasonable steps to ensure that the recipient does not breach the Australian Privacy Principles, as Australian Privacy Principle 8 requires, and satisfies itself that the recipient is subject to safeguards comparable to those in the New Zealand Privacy Act 2020, as Information Privacy Principle 12 requires. In practice this is done through the contractual terms Bastion puts in place with that recipient under its Third-Party Management Policy. Where comparable protection cannot reasonably be assured, Bastion does not proceed unless another lawful basis applies, such as your express informed consent.

Under section 16C of the Australian Privacy Act 1988, where Bastion discloses your personal information to an overseas recipient it generally remains accountable to you for that recipient's handling of it, as if Bastion had handled it itself. Sending your personal information overseas does not move Bastion's responsibility for it.

Where Bastion holds your personal information in capacity (b), any overseas storage or processing is determined by the engagement with the customer, and the customer is the party that decides it.

Security of Personal Information

Your personal information is stored in a way that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure. Bastion classifies personal information under its Data Management Policy and applies that policy's handling controls, including encryption at rest and in transit, restricted access on a need-to-know basis and monitoring of access to the systems that hold it.

Retention and Disposal

Bastion retains your personal information only as long as there is a genuine business, legal, regulatory or contractual need for it. When personal information is no longer needed for the purpose it was obtained for, Bastion takes reasonable steps to destroy it or permanently de-identify it.

Some categories of record must be kept for a minimum period set by law, and most personal information held in customer files is retained for a minimum of 7 years. Bastion's retention periods and secure disposal methods are set out in its Data Management Policy.

Personal information held in capacity (b) is retained and disposed of in accordance with the engagement contract and the customer's instructions.

Keeping Your Personal Information Accurate

It is important to Bastion that your personal information is accurate, complete and up to date, and Bastion takes reasonable steps to keep it that way. If you find that the information Bastion holds about you is inaccurate or out of date, please tell Bastion as soon as practicable so its records can be corrected.

Your Privacy Rights

You have the right to be told what personal information Bastion holds about you, to ask for access to it, to ask for it to be corrected and to ask Bastion to delete personal information it no longer has a genuine need to hold. These rights are given to you by the New Zealand Privacy Act 2020 and the Australian Privacy Act 1988, and they are subject to the exceptions those Acts set out.

- **Where to send a request:** requests should be sent to Bastion in writing using the details under Privacy Enquiries and Complaints, below. Where your request concerns personal information Bastion holds in capacity (b), Bastion will refer it as described in The Capacity in Which Bastion Holds Your Personal Information, above.
- **How long it takes:** for personal information Bastion holds in capacity (a), Bastion will decide on your request and tell you its decision as soon as reasonably practicable, and in any case no later than 20 working days after receiving it. This is the statutory timeframe under section 40 of the New Zealand Privacy Act 2020, and Bastion applies it in Australia as well rather than treating the two jurisdictions differently. Where a request is granted, the information or the correction follows promptly after that decision.
- **Proving who you are:** to protect your personal information, Bastion may ask you for reasonable proof of identity before it releases information or acts on a request.
- **Fees:** Bastion does not charge a fee for making an access, correction or deletion request. A reasonable administrative fee may apply to the cost of providing a copy of your personal information, and only where responding requires a substantial or unusual amount of time or cost.
- **If Bastion declines:** Bastion may decline part or all of a request only where an exception under privacy law applies, for example where granting it would reveal another person's personal information, or where legal privilege, trade secrets or a law enforcement exception applies. If Bastion declines, it will tell you why, and it will tell you that you may ask the Office of the Privacy Commissioner (New Zealand) or the Office of the Australian Information Commissioner, as applicable, to review that decision.
- **Deletion:** where Bastion agrees to delete your personal information, it does so using the secure disposal methods in its Data Management Policy, except where it has a legal, regulatory or contractual reason to keep it, such as a legal hold or a statutory minimum retention period. Bastion keeps a record of deletion requests and of the action it took on them.

Privacy Breaches

Bastion investigates any suspected or confirmed privacy breach under its Incident Response Plan, and acts to contain it and limit further disclosure.

Bastion assesses whether the breach has caused, or is likely to cause, serious harm to one or more individuals. It makes that assessment for personal information it holds in either capacity. Where the assessment is that serious harm has been caused or is likely, Bastion notifies the regulator and the affected individuals:

- **In Australia:** under the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act 1988, Bastion notifies the Office of the Australian Information Commissioner and the affected individuals as soon as practicable after forming a reasonable belief that an eligible data breach has occurred. Where Bastion has grounds only to suspect one, it completes its assessment as soon as practicable and within the 30 day statutory limit at the latest. That limit is an outer bound on a reasonable and expeditious assessment, not an entitlement to take the time; Bastion's own internal deadline is materially shorter.
- **In New Zealand:** under the Privacy Act 2020, Bastion notifies the Office of the Privacy Commissioner and the affected individuals as soon as practicable after becoming aware that a notifiable privacy breach has occurred. The Act sets no fixed number of days, and Bastion applies the same operational standard as in Australia rather than a looser one.

Where individuals in both countries are affected, both regulators are notified. A notification will tell you what happened, what personal information was involved, what Bastion is doing about it and what you can do to protect yourself.

Bastion records each privacy breach it identifies and the assessment made on it, including where the assessment is that the breach is not notifiable. The operational detail, including Bastion's internal assessment deadlines, is in its Incident Response Plan.

Where Bastion holds the affected personal information in capacity (b), Bastion still makes that assessment and still decides whether notification is required. Bastion tells the organisation that engaged it as soon as practicable, consults it on the assessment and agrees with it who notifies affected individuals, which is normally that organisation because it holds the relationship with them. Where agreement cannot be reached in the time available, Bastion acts on its own assessment.

Cookies and Website Analytics

Bastion uses cookies and website analytics to help personalise your online experience. Cookies are mainly used to provide access convenience. Bastion's websites keep track of the pages you visit within them so that Bastion can understand which of its services are of interest and speed up subsequent visits by remembering information you have previously entered.

That information may also be used to deliver tailored content and advertising to you where your browsing behaviour indicates you are interested in a particular subject area, both within Bastion's own websites and through the third-party advertising and analytics platforms Bastion uses.

You can accept or decline cookies. Most web browsers accept cookies automatically, but you can usually change your browser settings to decline them. If you decline cookies, you may not be able to use all the interactive features of Bastion's websites. The advertising and analytics platforms Bastion uses also provide their own opt-out controls.

Changes to This Policy

Bastion may update this policy from time to time to reflect changes in its business, in customer feedback or in applicable law. The current version is always the one published by Bastion, and you are encouraged to review it periodically.

Privacy Enquiries and Complaints

If you have a privacy enquiry, want to make a request about your personal information or wish to complain about how Bastion has handled your personal information, please contact Bastion in writing at support@cythera.com.au.

Written enquiries may also be sent by post to either of Bastion's offices:

- **Australia:** Level 10, 628 Bourke Street, Melbourne VIC 3000
- **New Zealand:** Level 8, 10 Brandon Street, Wellington 6011

Complaints are handled by Bastion's Privacy Officer, a role held by its Chief Information Security Officer. Please include your contact details, a description of your concern and what you would like Bastion to do about it. Bastion will acknowledge your complaint within 5 working days, investigate it, and give you a written response within 30 days of receiving it or, if it needs longer, tell you why and when you can expect a response. If you are not satisfied with that response, you may ask for it to be reviewed by Bastion's Executive Leadership Team. If you are still not satisfied, you may complain to the Office of the Privacy Commissioner in New Zealand (privacy.org.nz) or the Office of the Australian Information Commissioner in Australia (oaic.gov.au).

Policy Violation

All Bastion personnel (including employees, contractors and applicable third parties) must maintain the security, confidentiality, availability, integrity and privacy of Bastion assets. Any known violations of this policy should be reported to a direct manager and/or the CISO for escalation.

Violations of ISMS policies and procedures may be considered serious breaches of trust, which can result in disciplinary action up to and including termination of employment or contract, and prosecution in accordance with applicable laws and regulations.

Related Documents

Document Name	Purpose
Data Management Policy	Sets out Bastion's internal privacy obligations, including the capacity in which personal information is held, individual rights request handling, Privacy Impact Assessments, and the classification, handling, retention and disposal controls that apply to personal information.
Third-Party Management Policy	Sets out the supplier due diligence, contractual and ongoing assessment requirements applied before personal information is shared with, or processed by, a third party.
Incident Response Plan	Sets out how a suspected or confirmed privacy breach is detected, contained, assessed and responded to.
Information Security Policy	Sets out Bastion's overarching information security requirements.
Access Control Policy	Sets out the access governance controls that limit who can access systems and records holding personal information.

Document Control

Roles and Responsibilities

This policy is reviewed in line with the Bastion Security Group ISMS Framework, at a minimum annually or sooner if there is a material change to Bastion's process, operating environment or applicable legislation or regulation. The following information security roles and responsibilities are defined and allocated:

Role	Allocated to
Policy owner and approver. Approving this policy according to company and industry standards and ensuring organisational adherence.	Executive Leadership Team
Policy editor and implementer. Creating and maintaining the relevance of this policy and supervising its implementation, including coordinating individual rights requests and privacy breach assessment, and acting as Privacy Officer, including handling privacy complaints.	Chief Information Security Officer
Operational governance. Providing ongoing oversight of this policy's operation.	Head of Governance, Risk & Compliance

Version History

#	Date	People	Description
0.1	2026-09-08	Mark Terrill, CISO	Initial version, based on Cythera's existing Privacy Policy, Bastion's Privacy Policy v0.1 draft and Vanta's Privacy Policy taxonomy
1.0	2026-10-26	Euan Prentice, Executive Director	Formal approval