Sambe Consulting

IT Security and Privacy Policy

Document compiled by: Shaila Jivan
Information Officer: Shaila Jivan

Contents

Introduction

This Privacy and Security Policy sets out the policy of Sambe Consulting (hereinafter "Sambe") with regard to information that identifies the client and/or the client employees personally (known as 'personal information', but for purposes of this policy we will call "Personal Data") and other client information that is accessed by Sambe during the course of providing the Services (hereinafter "Client Data"). Within this policy document we will refer to Sambe as "we", "us" and/or "our".

By using any of our Services, you confirm that you have read, understood, and agreed to this Privacy and Security Policy.

Policy Statement

It is our policy to conduct all its business with transparency, integrity, and enforcing a zero-tolerance approach to bribery and corruption. We are committed to performing with honesty and acting professionally in all its business dealings and relationships. The nature of our business requires interaction with persons within various levels of multi-national client companies, small companies, and third-party service providers.

Security

Due to the fact that we are committed to ensuring that the privacy of their clients is protected, we make use of Microsoft Azure cloud services when storing any Personal Data and Client Data.

We take reasonable steps to protect the Personal Data and Client Data accessed in the course of providing the Services from loss, misuse, unauthorised access, disclosure, alteration, or destruction. No Internet or e-mail transmission is, however, fully secure or error free; any such transmission is accordingly at the client's own risk. Please keep this in mind when disclosing any Personal Data and Client Data to us by email. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Personal Data

We are the data controller under South Africa's Protection of Personal Information Act of 2013 ("POPI"). We conform to POPI in terms of the collection, use, and retention of Personal Data.

When you interact with us through the Services, we may collect and be given access to minimal Personal Data and other information from you and/or your employees, which typically includes your and/or your employees':

(i) name
(ii) telephone number
(iii) email address; and
(iv) any other personal information which you give us in connection with the Services.

By voluntarily providing us with access to Personal Data, you are consenting to our use of it in connection with the rendering of Services and in accordance with this Privacy and Security Policy.

We are not in the business of selling your Personal Data. We consider this information to be a vital part of our relationship with you. There are, however, certain circumstances in which we may share your Personal Data with certain third parties, as set out below:

On occasion, we will engage other service providers to perform certain business-related functions. When this happens, we only provide them with the information that they need to perform their specific function and they are subject to the terms and conditions of this Privacy and Security Policy.

Legal Requirements: we may disclose your Personal Data if required to do so by law or if we in good faith believe that such action is necessary to (i) comply with a legal obligation, (ii) protect and defend the rights or property of Sambe, (iii) act in urgent circumstances to protect the personal safety of users of the Services or the public, or (iv) protect against legal liability.

POPI gives you the right to access Personal Data held about you and/or your employees. Any access request may be subject to a small administrative fee to meet our costs in providing you with details of the information we hold about you. You may also email our Information Officer, Shaila Jivan at admin@sambe.co.za to request that we delete your Personal Data. We will use commercially reasonable efforts to honour your request.

Client Data

We shall have the right to access Client Data from time to time for the purposes of providing the Service. This Client Data can include any offline or online data that makes a person identifiable such as names, surnames, addresses, etc. As previously noted, we shall collect the Client Data in a transparent way and reasonably endeavour to ensure that no Client Data is accessed in an unauthorised manner for the duration of the provision of the Services. We shall promptly inform the Client if any Client Data has been accessed in an unauthorised manner or if we suspect that such access has occurred.

We shall securely destroy all Client Data upon the expiry of 90 (ninety) days from the date of completion or termination of the Services.

Once Client Data is made available to us, the following rules apply.

The data will be:

- Accurate and kept up-to-date.
- Collected fairly and for lawful purposes only.
- Processed by Sambe within its legal and moral boundaries.
- Protected against any unauthorised or illegal access by internal or external parties.

The data will not be:

- Communicated informally.
- Stored for more than a specified amount of time.
- Transferred to organisations or countries that do not have adequate data protection policies.
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities).

In addition to ways of handling the data, Sambe has direct obligations towards people and or clients to whom the data belongs. Specifically we must:

- Let people know which of their data is collected.
- Inform people about how we'll process their data.
- Inform people about who has access to their information.
- Have provisions in cases of lost, corrupted or compromised data.
- Allow people to request that we modify, erase, reduce or correct data contained in our databases.

Data Protection and Privacy

We collect, use, store and transfer information for legitimate and relevant employment, business management, client service and related processes and purposes in accordance with Sambe's Privacy Policy. These processes and purposes may include the transfer of the information within Sambe, between Sambe and its client, and to third parties where necessary for the above-mentioned processes and purposes.

Information Security

We handle various forms of client information, including confidential information, trade secrets and Intellectual Property. There is an obligation on Sambe and all staff to identify risks. And carefully process all forms of information to avoid information loss or damage and thereby to avoid serious reputational, financial, and legal risk to Sambe and its clients.

Back-Up Protocols

Daily back-ups of WIP are a requirement and failure to comply may result in disciplinary actions. Regardless of the type of work being performed – Sambe projects delivery, support or secondments, have to comply with the Sambe Back-Up protocols or utilise the resources in place at the client site. Additionally, all staff must ensure that all client data privacy policies are adhered to. Staff need to make of a point of getting clarity from the client if uncertain about what is expected of them in terms of their privacy policy.

General

The Services and our business may change from time to time. As a result, it may be necessary for us to make changes to this Privacy and Security Policy. We will highlight to you any material changes that we make. Your continued use of the Services after any changes or revisions to this Privacy Policy shall indicate your agreement with the revised terms.

Please also feel free to contact us if you have any questions about our Privacy and Security Policy. You may contact us on admin@sambe.co.za.

This Policy applies to all directors, employees (whether permanent, fixed term or temporary), consultants, contractors/sub-contractors, agency staff, affiliates and business development officers of Sambe.

Where any policy adopted by Sambe conflicts in any way with this Policy, then the policy providing the greatest level of protection against privacy, bribery, corruption and conflicts of interest shall prevail. This policy is in addition to and not a replacement of any existing policy governing privacy, anti-bribery, corruption or conflicts of interest.

Actions

To exercise data protection, we are committed to:

- Restrict and monitor access to sensitive data.
- Develop transparent data collection procedures.
- Train employees in online privacy and security measures.
- Build secure networks to protect online data from cyberattacks.
- Establish clear procedures for reporting privacy breaches or data misuse.
- Include contract clauses or communicate statements on how data is handled.
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation etc.).

Disaster Recovery Plan

- To minimise interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimise the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

Disaster Action Checklist

Plan initiation:

- Notify senior management and client.
- Contact and set up disaster recovery team.
- Determine degree of disaster.
- Implement proper application recovery plan dependent on extent of disaster.
- Monitor progress.
- Contact backup site and establish schedules.
- Contact all other necessary personnel–both user and data processing.
- Contact vendors–both hardware and software.
- Notify users of the disruption of service.

Follow-up checklist:

- List teams and tasks of each.
- Set up transportation to and from backup site, if necessary.
- List all personnel and their telephone numbers.
- Establish user participation plan.
- Determine applications to be run and in what sequence.
- Identify number of workstations needed.
- Check out any off-line equipment needs for each application.
- Check on forms needed for each application.
- Check all data being taken to backup site before leaving and leave inventory profile at home location.
- Set up primary vendors for assistance with problems incurred during emergency.
- Plan for transportation of any additional items needed at backup site.
- Take copies of system and operational documentation and procedural manuals.
- Ensure that all personnel involved know their tasks.
- Notify insurance companies.

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action. See Handbook for disciplinary actions.