Sambe Consulting

IT Security and Privacy Policy

Updated August 2021

M +27 (0) 82 334 6562 **T** +27 (0) 11 052 2820 **F** +27 (0) 11 052 2800 **E** info@sambe.co.za **A** 1 Maxwell Dr, Sunninghill, 2191, South Africa **A** P.O. Box 129, Lenasia, 1827 www.sambeconsulting.com

Contents

Introduction

This Privacy and Security Policy sets out the policy of Sambe Consulting with regards to information that identifies the client and/or the client employees or customers 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 Consulting during the course of providing the Services (hereinafter "Client Data"). Within this policy document we will refer to Sambe Consulting as "we", "us" and/or "our".

By providing or 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 our 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 our 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 our clients is protected, we make use of Microsoft Azure cloud services or on-premises servers when storing any Personal Data and Client Data.

We take reasonable steps to protect the Personal Data and Client Data accessed while providing the Services from loss, misuse, unauthorized 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 client information, we will use strict procedures and security features to try to prevent unauthorized access.

Personal Data

Sambe Consulting is classified as a 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 and Client Data. Our Privacy Officer is the Chief Operating Officer.

As part of our Service offering, we may collect and be given access to Personal and Client Data which typically includes:

(i) Name
(ii) Telephone number
(iii) ID Number
(iv) Email address; and
(v) any other personal information which you give us in connection with the Services.

By voluntarily providing us with access to Personal Data, our clients 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 Personal Data. We consider this information to be a vital part of our relationship with our clients. There are, however, certain circumstances in which we may share Personal Data with certain third parties, as set out below:

On occasion, we 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 also 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 Consulting, (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. 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 us at info@sambe.co.za to request that we delete your Personal Data. We will use commercially reasonable efforts to honour your request.

Client Data

We have the right to access Personal Data and Client Data from time to time for the purposes of providing the Service. As previously noted, we will reasonably endeavor to ensure that no Personal Data and Client Data is accessed in an unauthorised manner for the duration of the provision of the Services. We will promptly inform the client if any Personal Data and Client Data has been:

- accessed in an unauthorised manner or if we suspect that such access has occurred.
- Lost or shared in error.

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

Data Protection and Privacy

We collect, use, store and transfer information for legitimate and relevant employment, business management, client services and related processes and purposes in accordance with our Privacy Policy.

These processes and purposes may include the transfer of the information within Sambe Consulting, between Sambe Consulting and our 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 us and all our 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 us and our clients.

Back-Up Protocols

Daily back-ups of WIP are a requirement of all our staff and failure to comply may result in disciplinary actions. Regardless of the type of work being performed – our project delivery, support or secondments, have to comply with our 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.

Disaster Recovery Plan

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize 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.

General

Our service offering 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 info@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 Consulting.

Where any policy adopted by us 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.