ServCraft

HELPING INSTALLATION AND SERVICE TEAMS THRIVE

SERVCRAFT POPI COMPLIANCE

& Data Integrity

Job Management Software in the Cloud

ServCraft's mobile and cloud software platform will help you grow your business and make more money from happier customers and more efficient processes

Daniyel Falk
daniyel@servcraft.co.za
27 June 2021

Table of Contents

1 Introduction

This document describes our policies and procedures that have been put in place to ensure POPI compliance and data integrity to keep you and your customer data safe while using ServCraft.

ServCraft adheres specifically to

- CPA Section 11
- Protection of Personal Information ACT (POPI)

Our terms and conditions are accessible on our website. https://www.servcraft.co.za

Terms of use https://www.servcraft.co.za/terms-of-use/

Privacy Policy https://www.servcraft.co.za/privacy-policy/

1.1 Information Request & Contact Details

If your personal information changes (e.g. your email address or cell phone number), or if you no longer wish to use or access the service, ServCraft supports you to correct, update, or remove the personal information that you provided. This can be done by contacting us.

In the event that a data subject either (i.e. a customer contact in your list) would like access to their data, requests must be submitted to us in writing. Requests for personal information will be handled in accordance with the POPI Act.

Our Information Office is, Daniyel Falk (Director).

For any information or removal requests pertaining to POPI, please email popi@servcraft.co.za

We have a 72-hour response time in relation to emails sent to this address.

Alternatively, call 087 813 1137 for additional help or escalations.

2 Technology Setup

2.1 Databases

ServCraft uses SQL based relationship databases to house its data. Both primary and second (replicated) Databases sit behind firewalls and are password protected. Access to these databases is governed by our internal staff policies. Replicated databases reside in Microsoft Azure platform.

Data is encrypted at rest using TDE (Transparent data encryption with AES 256), it is stored in the files of the database management system, Microsoft SQL Server and cannot be accessed from the database unless the necessary login details are correct. The database servers exist behind a secure firewall and root access to the servers is not possible.

We utilize multiple databases and share our data. Sharding of data is a logical separation of Customers data within a single database. The fundamental code of ServCraft has been carefully constructed to ensure the integrity of this logical separation as well as ensuring that customers data is only accessed with the correct login access for an individual who has been given access to that data.

2.2 Application

ServCraft, being a cloud-based application, is housed within Web Servers. These web servers are protected by firewalls. Access is limited to these servers with administration control granted at the top levels of the company. They are also governed and protected by our internal staff policies.

We do not allow scripts to be executed in any location that the application has access to.

2.3 Other Data

We use Amazon Web Services (AWS) S3 in order to store files and videos that are attached to ServCraft by our customers. Amazon is a well-known international service provider that complies to the highest standards in terms of encrypting and protecting standards. They comply with strict international standards notably GDPR. One can find additional information about their compliance at https://aws.amazon.com/compliance/gdpr-center/

ServCraft utilizes S3 to store files in two ways.

- The first is public accessibility, this is only used for our customers Logos, in a similar fashion to how their logos would be available on their own company websites.
- The second is used for all other files and is only accessible through a private URL that is exclusively generated within the ServCraft platform. I.e. one must have valid attachment access through the ServCraft platform in order to access these files.

Other document files (such as Job card or Quote PDFs) are generated on demand either through viewing them from ServCraft's frontend or when sending email communication as attachments.

2.4 Backup

The Primary ServCraft Databases are backed up daily at night. Our current policy is to ship the latest two backups to a protected off site provider – we are currently using Google to house these offsite backups. In addition, we back up off our replicated databases on Azure with a 7 days PITR and a 8 Week LTR Policy. Google and internal servers are projected by passwords and firewalls. Administration of these passwords is governed by our internal staff policies.

2.5 Service Providers

ServCraft utilizes a number of Service providers. We select these service providers because they are international, well known and comply to the highest international standards including GDPR (General Data Protection Regulation) and Popia.

Our current list of Primary Service Providers they pertain to the storage or handling of data are

- Amazon
  - https://aws.amazon.com/compliance/gdpr-center/
- Google Cloud and Workspaces
  - https://cloud.google.com/security/gdpr
- Microsoft Azure
- SendGrid (Twillio)
  - https://sendgrid.com/resource/general-data-protection-regulation-2/
- SMSPortal
  - https://docs.smsportal.com/docs/popia-act-2013
- Xneelo
  - https://xneelo.co.za/help-centre/products-and-services/data-protection/

2.6 Primary Data hosting

Our current hosting is with Xneelo. Physical access is highly restricted. Our servers are managed by our own internal staff, as such there is no access for third parties.

2.7 Mobile App

ServCraft has the ability to run offline on its mobile app. As a result of this functionality a portion of data will be synchronized to either Android or Apple Device. This subset of data is

- Limited to the customer's particular data which is defined by authenticated login access
- Limited to the access restrictions for that particular user

The database is not accessible locally without having authenticated access from within the app.

2.8 SSL

All data transfer between the utilized Secure Sockets Layer which means that data is encrypted during transmission.

2.9 System Monitoring

ServCraft uses a combination of automated monitoring and manual oversight to ensure services remain intact and secure.

2.10 Application Access Control and Audit Logs

We use industry-standard procedures and protocols to ensure the highest levels of access control.

All internal and external access to the application is logged in our Audit Logs. All changes on the system are logged directly in the database and replicated with the core data.

2.10.1 Secure Login

We take every possible precaution to ensure that only authorised parties can log into the system.

2.10.2 Passwords

For security reasons we do not share the specifics of application password encryption. At a high level, our passwords are encrypted, and only forward validation is possible.

All passwords are encrypted, including those used for API integrations. The passwords are encrypted in such a way that they can't be decrypted.

Users can change their password within the application, using the 'forgot password' function. Additionally, an Administrator or Owner of a system may change a user's password but only if that user belongs to that customer.

2.10.3 Brute Force Attack Prevention

Our servers sit behind hosting services that detect and limit the effectiveness of a brute force attack.

2.11 Service Logs

Text logs are created locally for error monitoring or general service health. Log files are deleted automatically within 7 days and reside exclusively on our primary Servers.

3 Disaster Recovery (DR)

The database replication is core to our disaster recovery plan whereby we can bring offline servers within the Microsoft Azure platform online and connect to our replicated databases.

All DR infrastructure privacy and security is congruent with other services and Servers currently in operation. Staff access is governed by our internal policies and strictly adhered to.

4 Internal Controls

4.1 Physical Access

All servers reside in hosting centres and no physical access is granted without authorization at the top levels of the business. We work remotely and no documents or data pertaining to our Customers would be found at any physical location besides company computers. The protection of this information is governed by our staff policies and procedures.

4.2 ServCraft Staff Policies and Procedures

In general, the client is assigned a senior account manager and they will have access to client data in order to support their clients. These employees are moderated by their employment contracts, and the gravity of their access rights is reinforced during induction. Access is physically restricted to the ServCraft office through IP restriction; only staff on our IP network can access client data. Furthermore, staff members can only access client data if they have permission to do so.

All ServCraft staff and contractors attest to terms and conditions that specifically outline privacy, information security, and confidentiality. ServCraft staff are also trained yearly on the following:

- General procedures
- Paper records
- Email and personal productivity software
- Electronic remote access
- Laptops/notebooks
- Mobile storage devices
- Data transfer
- Monitoring
- Breach management

4.3 Employee, Contractor, and Service Provider Procedures

Background checks that include a criminal record and credit check are conducted on all staff and contractors before they are hired.

Personnel who retire, transfer from any internal department, resign etc. are removed immediately from mailing lists and access control lists. Relevant changes also occur when staff transfer to other internal assignments.

New staff are trained before being allowed to access confidential or personal files.

Contractors, consultants, and external service providers employed by ServCraft are subject to a strict formal contract in line with the provisions of the POPI Act. The terms of the contract, and undertakings given, are reviewed and audited to ensure compliance.

ServCraft has an up-to-date Data Protection and Privacy Policy in relation to the use of any office technology and software (for example telephone, mobile phone, fax, email, internet, intranet, and remote access, etc.) by its staff. This policy is understood and signed by each user of such technology at ServCraft.

Staff ensures that callers to the office or other unauthorized persons are unable to view personal or sensitive information, whether held on paper documents or information displayed on PC monitors, etc.

All staff ensure that PCs are logged off or 'locked' when left unattended for any period of time. Where possible, staff is restricted from saving files to the local disk. Users are instructed to only save files to their allocated network or cloud drive.

4.4 ServCraft Policies and Controls for Unauthorised Access to Client Information

4.4.1 Paper records

Paper records and files containing personal data are handled in such a way as to restrict access to only those persons with business reasons to access them.

ServCraft shreds all paper records that contain confidential information. Other secure disposal methods are in place and properly used for confidential material not on paper.

Facsimile technology (fax machines) are not used.

Papers with confidential data are locked away when not in use.

4.4.2 Email and Personal Productivity Software

Standard unencrypted email is never used to transmit any data of a personal or sensitive nature. Clients that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted, either through file encryption or through the use of a secure email facility which will encrypt the data (including any attachments) being sent.

Where personal or sensitive data is held on applications and databases relevant security and access controls measures are in place.

4.4.3 Remote Access

When accessing this data remotely, it is done via a secure encrypted link via an SSL VPN tunnel with relevant access controls in place. Stringent security and access controls, such as strong passwords, are used for an additional layer of protection.

ServCraft ensures that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately with up-to-date anti-virus and anti-spyware software are allowed to remotely access centrally-held personal or sensitive data.

4.4.4 Laptops and Other Mobile Storage Devices

All mobile devices are password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. Passwords used to access PCs, applications, databases, etc. are of credible strength to deter password cracking or guessing attacks. Laptops are kept secure at all times.

Staff-owned devices, such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc, are restricted from connecting to ServerCraft-owned computers. ServCraft implements procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required.

When replacing or selling laptops, hard drives are formatted and cleaned with a hard drive degausser program.

4.4.5 Data Transmissions

Data transfers only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. In general, we do not employ manual data transfers using removable physical media (e.g. memory sticks, CDs, tapes, etc.). However, in the event it is absolutely necessary, any such encrypted media will be accompanied by a member of ServCraft staff delivered directly to, and be signed for, by the intended recipient.

4.4.6 General Monitoring

ServCraft ensures that all systems are protected by appropriate firewall technologies and that this technology is kept up-to-date, and is sufficient to meet emerging threats.

Access to files containing personal data is monitored by supervisors on an ongoing basis. Staff is made aware that this is being done.

ServCraft also takes the below precautions:

- Privileges are allocated on a need-to-use basis, and only after a formal authorisation process
- User access rights are reviewed at regular intervals
- Users are advised on how to select and maintain secure passwords
- Users and sub-contractors are made aware of the security requirements and procedures for protecting unattended equipment
- Inactive sessions are shut down after a defined period of inactivity

4.4.7 Reports & Incidents

We have a breach management plan to follow should an incident occur. There are five elements:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

4.4.8 Identification and Classification

Though ServCraft does everything technologically to ensure data security, we have also put in place procedures that will allow any staff member to report an information security incident. Staff are aware they should report such an incident to the Information Officer.

This allows for early recognition of the incident so that it can be dealt with in the most appropriate manner. The report is then reviewed by the Information Officer to confirm if a breach has actually occurred.

4.4.9 Containment and Recovery

This step limits the scope and impact of the breach of data protection procedures. If a breach occurs, the Information Officer:

- Investigates the breach and ensures that the appropriate resources are made available for the investigation.
- Establishes who in the organisation needs to be made aware of the breach and begins the containment exercise.
- Establishes whether there is anything that can be done to recover losses and limits the damage the breach can cause.

4.4.10 Risk Assessment

In assessing the risk arising from a data security breach, the Information Officer will consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be.

4.4.11 Notification of Breaches

If inappropriate release/loss of personal data occurs it is reported immediately, both internally and to the Data Protection Office and, if appropriate in the circumstances, to the persons whose data it is. When notifying individuals, ServCraft will consider using the most appropriate medium to do so.

4.4.12 Evaluation and Response

Subsequent to any information security breach a thorough review of the incident will occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.