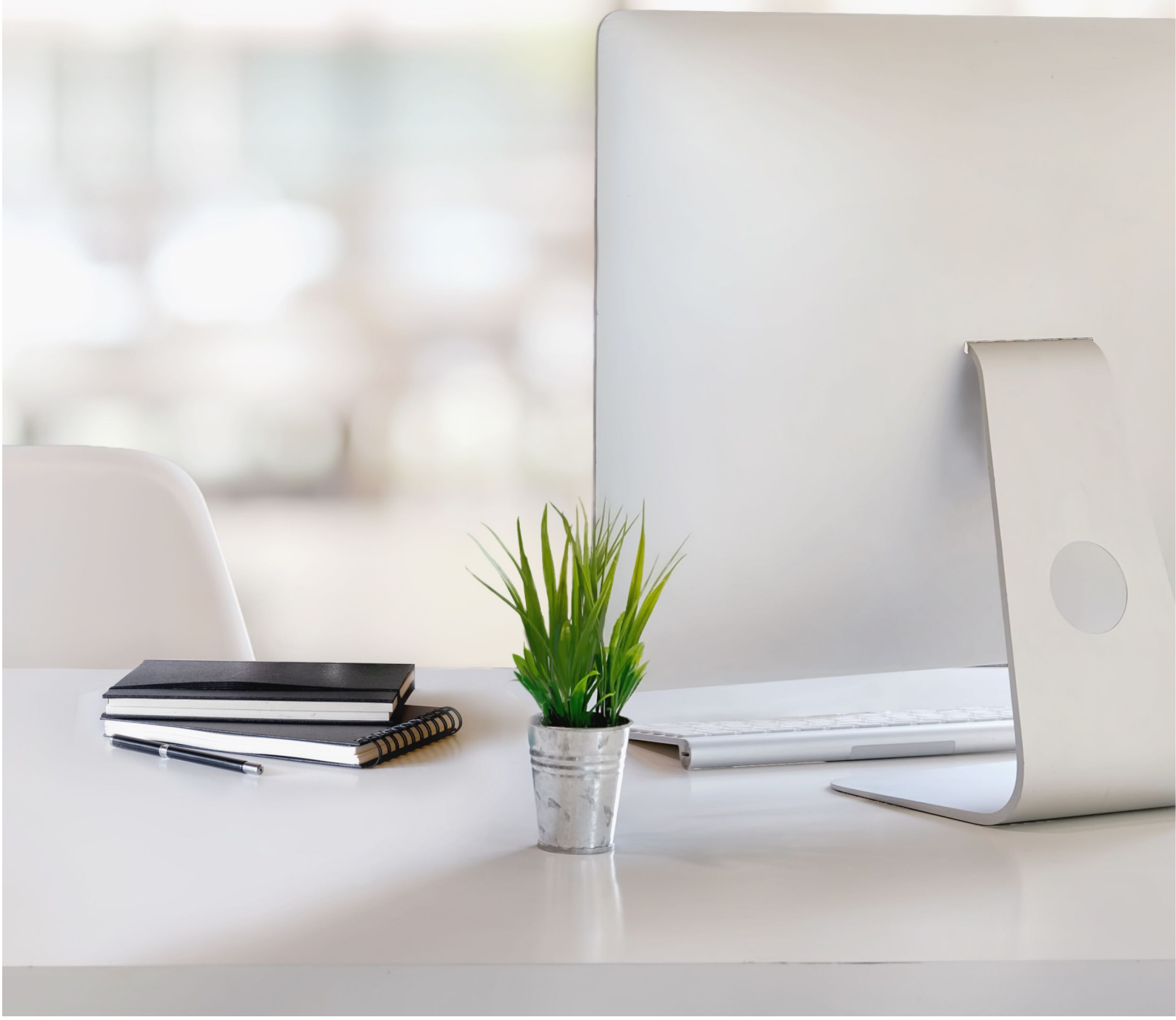
dotcube

Privacy & Security Policy
(POPI)



PRIVACY AND SECURITY POLICY **(POPI)**

Introduction

Dot Cube (Pty) Ltd hereafter referred to “Dot Cube” believes that the responsible use of personal information is critical to its business objectives and reputation and we are committed to protecting your personal information. It is important to us that personal information is used appropriately, transparently, securely and in accordance with the Protection of Personal Information Act, 4 of 2013. The purpose of this policy is to set out the safeguards and procedures implemented to ensure the protection of personal information as required by POPI. This policy also aims to exercise effective control over the use and retention of personal information we may obtain during the normal course of business and provide you with peace of mind when it comes to your personal information.

Definitions

“ECTA” refers to Electronic Communications Act, 25 of 2002.

“Personal information” refers to all information considered to be or which may be considered to be personal information about an identifiable individual in terms of Protection of Personal Information Act 4 of 2013 or other relevant South African legislation.

“Dot Cube” or “DotCube” refers to Dot Cube (Pty) Ltd with registration number 2015/087445/07 a company incorporated in accordance with the laws of the Republic of South Africa.

“User, you or your” refers to any person who makes use of this website.

“Policy” refers to our Online Privacy Policy.

“POPI” refers to Protection of Personal Information Act, 4 of 2013.

Personal information collected

We will only process personal information if the purpose for which it will be processed is adequate, relevant and not excessive. The type of information we collect is only relevant for the provision of services to you as set out in our Terms of Use and will be processed for that purpose only. As far as possible, we will inform you when your personal information is required and whether the information is deemed optional. You are under no obligation to provide us

with your personal information. In some instances, not having your personal information will prevent us from providing you with our service and you will not be able to make full use of the website. Dot Cube aims to have agreements in place with all third party service providers and trusted partners to ensure a mutual understanding with regards to the protection of our client's personal information. Our service providers will be subject to the same regulations as applicable.

How we use your data

We will use your personal information to provide you with our service and to carry out transactions as requested. We will also periodically use your information to confirm, verify and update your details. We may use your information to conduct market or customer satisfaction research to allow continuous improvement on our solutions. Furthermore, your personal information may be used in connection with legal proceedings and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

How we may share your data

Dot Cube may disclose your personal information to any of its subsidiaries, joint venture companies and or approved third party service providers whose services or products you require use of. We have agreements in place to ensure compliance with confidentiality and privacy conditions. We will only share your data, without your written consent, under the following circumstances:

• Where disclosure is under compulsion of law;

• Where there is a duty to the public to disclose; and

• Where the interests of the company require disclosure.

We may also share your personal information with, and obtain information about you from third parties for the reasons already discussed. We may disclose your information where it may be deemed necessary in order to protect the legitimate rights of Dot Cube. All of the Dot Cube employees have a duty of confidentiality in relation to the company and our clients.

Retention

We store and keep your personal information for periods as prescribed in the applicable and relevant legislation and regulations. Only information as required in terms of legislation is stored and we adhere to strict procedure as far as destruction of information is concerned. Destruction of data includes, but is not limited to, anonymising and aggregation of personal information. Your rights Your rights to privacy and confidentiality are important to us. These rights are also protected by the Constitution, ECTA and POPI.

Cookies

We sometimes use cookies on this website to improve the user experience and ensure that it is functioning effectively. In order to provide you with a more personalised and responsive service we need to remember and store information about how you use the website. This is done using small text files called cookies. Cookies contain small amounts of information and are downloaded to your computer or other device by a server for the website. Your web browser sends these cookies back to the website on each subsequent visit so that it can recognise you and remember things like your user preferences. You can set your browser to notify you if cookies are to be transferred or to reject cookies, but this may prevent your use of some of our web pages. Whenever you use this website, information may be collected through the use of cookies and other technologies and by proceeding to use this website you agree to the use of cookies.

Security

Dot Cube has appropriate measures and controls in place to ensure that your personal information is adequately protected. We will also continuously review our security systems and protocols as new technology becomes available and in compliance with POPI. This policy has been put in place throughout Dot Cube and training on this policy and POPI will be conducted on an ongoing basis. Each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI. Every employee currently employed by Dot Cube will be required to sign an addendum to their employment contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI. Archived client information is stored at Dot Cube's office and access to

retrieve information is limited to authorised personnel. Third party service providers are required to sign a service level agreement guaranteeing their commitment to the protection of personal information.

Physical Security

Dot Cube's servers are hosted in the xneelo Samrand Data Centre (Gauteng). The Samrand Data Centre is our default hosting location. The facility is not in a direct flight path or low lying area and is centrally located between Johannesburg and Pretoria with a major power substation close by. A geotechnical audit has been done to ensure ground stability.

Surveillance

The Samrand data centre uses 45 internal and external surveillance cameras, as well as 10 perimeter cameras, which are strategically placed and monitored around the clock to ensure that all servers remain off-limits to anyone without security clearance. High-voltage security fences and a 24/7 security presence help to deter any opportunistic crimes.

Access Control

Customers, employees and contractors have varying levels of authorised access to different areas of the facility, controlled by high-tech biometric scanning systems, with 20 devices and pin-coded keypads.

Fire Prevention

The facility is custom-designed for low fire risk, with a Very Early Smoke Detection Apparatus (VESDA) installed to trigger alarms at even the slightest hint of smoke particles.

There are no flammable materials present in the 'white space' in the Data Centre and all cabling is fire-retardant.

Power Outages

An 11kV power supply from the municipal power utility energises a fault-tolerant, medium-voltage ring that powers two separate low-voltage 2MVA energy centres. These A- and B feeds power mission-critical infrastructure such as IT load, air conditioning, security systems and emergency lighting. They provide seamless electrical failover with their own emergency backup power systems in the event of a power failure.

The Samrand Data Centre has on-site fuel storage sufficient to run the generators for 7 days' continuously. The Samrand Data Centre UPS's provide always-on power, with battery standby time of 30 minutes.

Connectivity

The network is multi-homed with multiple uplinks via at least two Tier 1 upstream providers and peering partners. Should a network failure occur, traffic is automatically rerouted via alternate uplinks, significantly increasing our network resilience.

Connectivity is provided through diverse, redundant fibre routes connecting the facility to a 10Gbps fibre ring.

Network Security

Network level security consists of three main components:

1. DDoS mitigation
2. VLAN reverse path forwarding protection
3. Juniper firewall rules at the network edge and core

DDoS mitigation

A DDoS detection and mitigation system is deployed. DDoS attack traffic is diverted to a filter/scrubbing server that can distinguish between valid and malicious traffic. Malicious traffic is scrubbed off while valid traffic is re-injected into the network. The victim IP is not affected during the DDoS attack. DDoS detection and mitigation is fully automated and traffic diversion occurs automatically.

Small DDoS attacks are scrubbed locally in the data-centre by the mitigation system. For larger attacks, traffic is diverted to an international DDoS mitigation provider which then sends the clear traffic on to South Africa.

VLAN Reverse path forwarding protection

Reverse path forwarding protection is enabled for all VLANs in the Samrand Data Centre. This policy ensures that only the subnets allocated to a VLAN can generate traffic for that VLAN. This helps to mitigate two kinds of malicious traffic:

- Source-spoofed traffic where a host is sending out traffic for subnets that do not belong to the VLAN.
- Inter-VLAN subnet spoofing, where a host in one VLAN uses IP addresses from another VLAN using source-spoofing.

Juniper firewall rules

Firewall rules on the data centre network edge and at the core are used to protect the network in a number of ways:

- Rate-limiting of certain protocols to protect the network infrastructure.
- Blocking of certain protocols and destination IP addresses to protect operational systems.
- Restricting access to certain hosts and protocols to defined lists of source addresses.
- Blocking of abusive IP addresses and hosts.

Monitoring

All servers are monitored 24/7 for all critical services and hardware health. Our reactive system administrators react to monitoring alerts as they are identified and escalate issues to data centre staff or platform engineers.

Platform Security

Servers

Servers are designed to provide redundancy and reliability, including multi-core, multi-CPU systems, ECC (Error-Correcting Code) memory modules to detect and correct data corruption in real time and enterprise grade storage that includes hard disk and solid state drives.

All data is stored on dedicated, robust RAID storage arrays providing data redundancy and integrity.

Backups

All accounts are automatically backed up in the early hours of the morning. The backup includes all critical data required for disaster recovery.

Backups are made of the user's home directory as well as databases. The user's home directory will include site content, web logs and any mail that was on the server at the time that backup was completed.

Backups are retained as follows: This morning, yesterday morning, Sunday morning, morning of the 1st of this Month and the morning of the 1st of Last Month. Customers can request a restore of the backup. If you have critical data which you cannot afford to lose in the event of a disaster, keep a copy of your data locally (or at an alternate location) as well.

Logs (such as FTP, web server and mail logs) are normally kept for 60 days.

Hosting Servers System Software

We make use of WHM/cPanel Software running on CentOS 7.x. cPanel is a web hosting control panel software developed by cPanel, LLC. It provides a graphical interface (GUI) and automation tools designed to simplify the process of hosting a web site to the website owner or the "end user". It enables administration through a standard web browser using a three-tier structure.

Anti virus

All servers (which are Linux based) run anti-virus software which is updated as new virus definitions are released. Servers are scanned daily.

User passwords

All customer passwords are stored in a one-way encrypted format. We are not able to retrieve any passwords. Due to the broad technology implementation across our hosting software and platform, we employ a number of different password hashing algorithms e.g. bcrypt, sha-512. We implement industry standard practices for mitigating various password cracking methods.

Mail security

SSL is used for POP, IMAP and SMTP protocols for email, resulting in data encryption between our server and customers' mail programmes.

The use of strong passwords is enforced when creating or editing mailboxes via the mail admin tool.

The following measures are used to mitigate spam and malware:

- Anti-virus and anti-spam scanning occurs on all inbound email.
- Common malicious file extensions are blocked for both inbound and outbound email.
- Known malicious IP addresses are blocked by our firewall for incoming email.

Data protection

Data protection includes security and is a related topic.

Payment Data Security

Credit / debit card purchases for services are processed by the third-party vendor, Payfast. No credit / debit card information is submitted via our website or stored on any of our systems.

Other

Incident response

We have good incident response plans, procedures and practices in place that mean we respond to incidents or data breaches quickly and effectively.

Trust and Safety team

Our dedicated team monitor the hosting platform for any form of abuse such as compromised websites and mailboxes, network abuse and phishing attacks and take swift remedial steps. They also contribute towards adapting our systems to current trends in spam to ensure that our spam filtering service is effective.

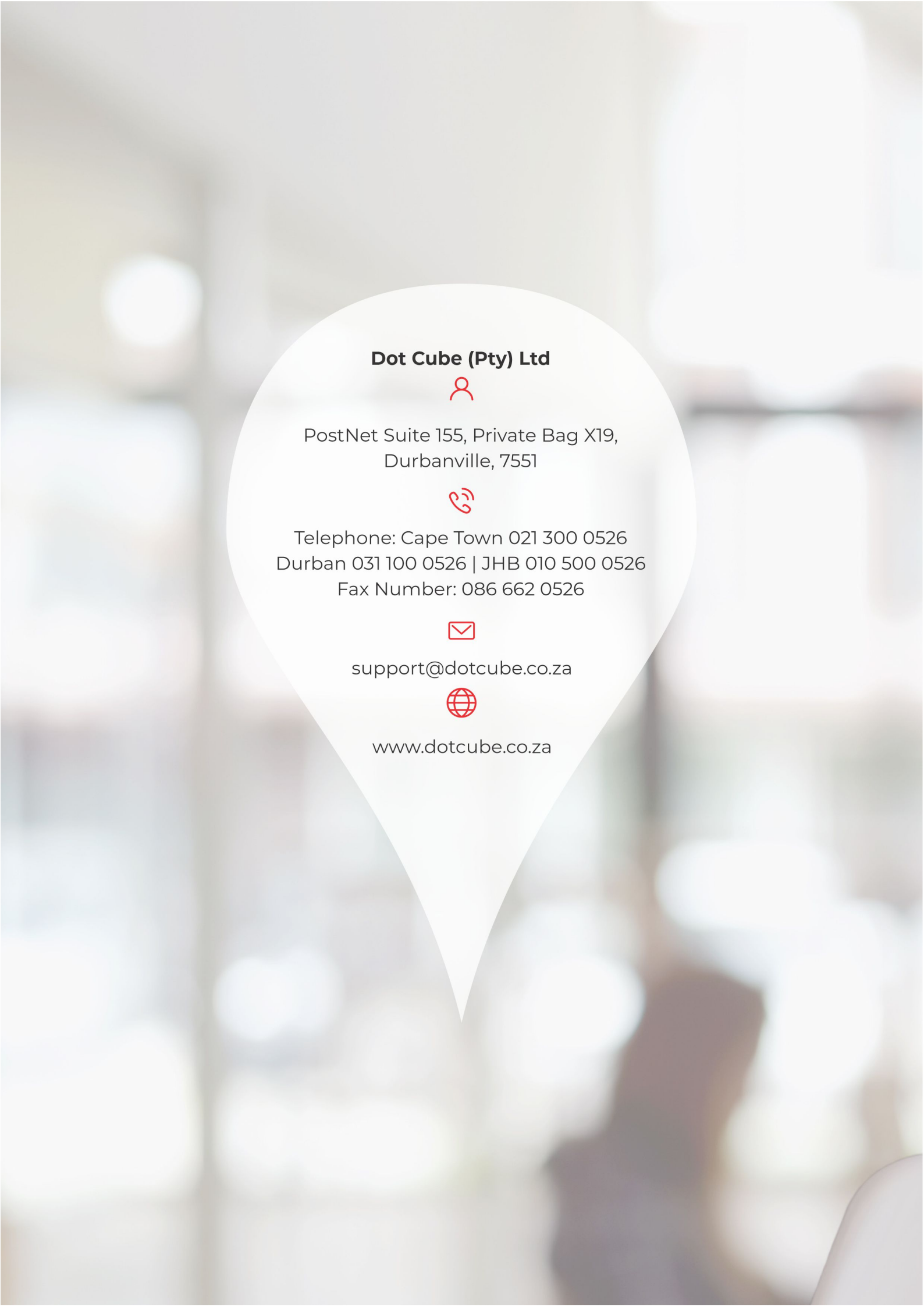
Customer responsibilities

While we care for the hosting infrastructure including the network and servers, it is our customers responsibility to keep their data and hosting account secure.

- Use secure passwords and store them safely
- Ensure sufficient security for your web applications
- Ensure that CMS' and plugins are always kept up-to-date

Updating of this policy

We reserve the right, in our sole discretion to update, modify or amend (including without limitation, by the addition of new terms and conditions) this Policy from time to time with or without notice. You therefore agree to review the policy whenever you visit our website for any such change. Save as expressly provided to the contrary in this policy, the amended version of the Policy shall supersede and replace all previous versions thereof.



Dot Cube (Pty) Ltd

PostNet Suite 155, Private Bag X19,
Durbanville, 7551

Telephone: Cape Town 021 300 0526
Durban 031 100 0526 | JHB 010 500 0526
Fax Number: 086 662 0526

support@dotcube.co.za

www.dotcube.co.za