Master Services Agreement:

Annexure E: Service Schedule - Hosted Website Services v8.0.0

This Service Schedule for **Hosted Website Services v8.0.0** (the "Service") replaces all previously signed / incorporated version(s) of the Service Schedule(s) for Hosted Website Services (if any) and forms part of the Master Services Agreement and Master Services Schedule. Its provisions are an integral part of the Master Services Agreement. Words and expressions defined in the General Conditions and Master Services Schedule shall (unless otherwise defined in this Services Schedule) bear the same meanings where used in this Service Schedule. In this Service Schedule the following words and phrases shall have the following meanings unless the context otherwise requires:

1. Interpretation

1.1. The clause headings contained herein are for reference purposes only and shall not be used in the interpretation of this agreement. Words which denote any one gender include the other gender, the singular includes the plural and vice versa, a reference to any person shall include natural persons, artificial persons and unincorporated entities and their successors-in-title and assigns. Any reference to a number of days excludes weekends and public holidays and shall be reckoned exclusively of the first and inclusively of the last day. Anything which is required to be done, performed or recorded in or reduced to writing (including but not limited to written requests, consents, directions and matters to be in writing) may be done, performed or reduce to writing provided by way of a data message, including but not limited to emails, telefax, and/or the DocuSign Process. In this Master Services Agreement, the following words and phrases shall have the following meanings unless the context otherwise requires:

1.2. Agreement - These General Terms and any specific terms that incorporate (include) MSA

1.3. Customer - Is any person identified on the application form for Services or in any addendum;

1.4. Customer Data - Any username, password or email address we give the Customer as part of the Services. This excludes Customer Domains we manage as part of the Services;

1.5. General Terms - The General Terms and conditions governing the contractual relationship between the parties, supplemented by the Specific Terms;

1.6. Our Hosting Terms - The General Terms, the Specific Terms, the Acceptable Use Policy, and Privacy Policy.

1.7. You or your - The Customer, including a legal entity (such as a company), who enters into an Agreement with Online Direct;

1.8. Specific Terms - The terms and conditions which supplement the General Terms and govern the use of individual Services (MSA)

2. Online Directs hosting terms

2.1 Online Direct make use of various hosting providers including but not limited to, Online Direct, Global Micro, Afrihost and RSAweb

2.2 These General Terms govern the contractual relationship between us, duly supplemented by the MSA.

2.3 Unless expressly provided to the contrary in our Hosting Terms, if there is a conflict in meaning, the following precedence ranking will apply (from highest to lowest): i. the MSA; ii. these General Terms; iii. the Acceptable Use Policy

3. Amendment to Our Hosting Terms

3.1 Online Direct reserves the right to make changes to Our Hosting Terms at any time without notice. An updated version of our Hosting Terms will be posted on the Website.

3.2 It is the customers responsibility as a diligent user to check any amended Hosting Terms posted on the Website.

3.3 If you object to any amended Hosting Terms, you are entitled to terminate your relationship with us under clause 14.

4. Monitoring

4.1 We monitor our hosting facilities, but not your specific activities. Where we have to intercept communications in accordance with the Regulation of Interception and Provision of Communication-Related Act, 70 of 2003 ("the Monitoring Act"), we will do this according to the requirements of the Monitoring Act.

4.2 With specific regard to the monitoring of content that is found on a website that belongs to counterpart and which is hosted by Online Direct, we have no knowledge of, nor interest in, Customer content hosted by us or published by us on your behalf using the Services and further we do not in any way contribute to or approve the content.

4.3 If however we determine that any content is in violation of any law (including the Films and Publications Act 65 of 1996) or of the Acceptable Use Policy, or if we receive a takedown notice from ISPA, as contemplated in section 77 of the Electronic Communications and Transactions Act 25 of 2002, we may:- ask you to remove, amend, or modify the content; -- terminate access to any Services or suspend or terminate any Services without notice; -- delete the offending content without notice; -- notify the relevant authorities of the existence of any content, make any back-up, archive, or other copies of any content; or -- take any further steps as required or requested by any authorities without notice.

4.4 We may disclose any content, material, or data (including any of your data) if required by law; lawfully asked to do so by any authorities, including the South African Police Services pursuant to a subpoena under section 205 of the Criminal Procedure Act 51 of 1977; or according to a judicial, administrative or governmental order. We do not have to give you notice.

4.5 You will have no recourse against us if we act under this clause and you accordingly waive your right to make any claim or demand, or to institute any legal proceedings against us.

5. Security

5.1 All Customer Data allocated to you is personal to you and you will be liable for any loss or damage you or third parties have suffered because of your actions or the actions of a person to whom you have disclosed your Customer Data.
5.2 You authorise us to act on any instruction given by or purporting to originate from you even if it becomes clear that both parties have been defrauded by someone else.
5.3 If any security violations are reasonably believed to have occurred in connection with your account, we will investigate and, if necessary, change the relevant Customer Data, including access codes and passwords, and notify you immediately.
5.4 You must tell us immediately if any other person gains access to your Customer Data by logging a ticket via our standard escalation procedure and following up with a phone call if need be. You indemnify us (hold us harmless) against any claim arising from: your disclosure of your Customer Data to a third person; the use of the Customer Data by a third person; or any resulting action by you or a third party.
5.5 We reserve the right to take any action we find necessary to preserve the security and reliable operation of our infrastructure. You may not do anything (or permit anything to be done) that will compromise our security.
5.6 We have systems in place to assist our critical technical infrastructure to recover from a natural or human induced disaster. However, we do not specify any recovery time and are not liable for any loss or damage you suffer as a result of a disaster. You must make back-ups of your data. Nothing contained in Our Hosting Terms will be seen as a representation that any back-ups of data we have implemented will be successful or in any way will assist with disaster recovery.

6. Warranties

6.1 We warrant that our network providers have the facilities, infrastructure, capacity, and capability to provide the Services.
6.2 Despite this warranty, the Services are provided “as is” and “as available”. No warranty of any kind is given, whether express or implied, including warranties of merchantability, title, or non-infringement, except where such a warranty is specifically required by law.

7. Intellectual Property Rights

7.1. You must comply with all laws that apply to any intellectual property.
7.2. You must get our prior written approval before using any of our marks.
7.3. You grant us non-exclusive licence to use your marks so that we may exercise our rights or fulfil our obligations under Our Hosting Terms.
7.4. Other than as specifically provided for in Our Hosting Terms, we retain all Intellectual Property Rights employed in or otherwise related to our network infrastructure, business and the provision of any of the Services under Our Hosting Terms.

8. Customer Indemnities

8.1. You indemnify (hold us harmless) from any liability arising from civil or criminal proceedings instituted against us or for any loss or damage you or a third party have suffered because of any interruption or unavailability of the Services.
8.2. You indemnify us and hold us harmless against all losses you have suffered or actions against us as a result of: the use of the Services, or any downtime, outage, degradation of the network, interruption in or unavailability of the Services. Included within the range of downtime, outage, degradation of the network, interruption, or unavailability of the Services is any of the following: software or hardware service, repairs, maintenance, upgrades, modification, alterations, replacement or relocation of premises affecting the Services, non-performance or unavailability of any of the services given by an electronic communications network or service provider, including, line failure, or in any international services or remote mail Servers, non-performance or unavailability of external communications networks to which you or our network infrastructure is connected, and repairs, maintenance, upgrades, modifications, alterations or replacement of any hardware forming part of the Services, or any faults or defects in the hardware.
8.3. If we are sued for something that you have indemnified us for, you will take our place in the law suit or be liable to pay us back for any costs, damages and expenses including attorneys’ fees on the attorney and own client scale (you will be liable to pay our attorney’s fees finally awarded against us by a court or agreed to in a written settlement agreement, provided that we notify you in writing as soon as we become aware of the indemnified claim so you can take steps to contest it; you may assume sole control of the defence of the claim or related settlement negotiations; and we will give you, at your expense, with the assistance, information, and authority necessary to enable you to perform your obligations under this clause.
8.4. You indemnify us against any loss or damage that Online Direct may suffer because of your actions.

9. Suspension of the Services

9.1 Online Direct may temporarily suspend its Service to repair, maintain, upgrade, modify, replace or improve any of its Services. Where circumstances permit, Online Direct will provide prior notice of any service suspension to Customers. However, Online Direct will not be held liable for any resulting loss or damage suffered as a result of the service suspension**.**

10. Termination

10.1. Online Direct may terminate any Services on five days written notice to you.

10.2. Breach: If you breach any of Our Hosting Terms, we may, without prejudice to any other rights that Online Direct may have and without notice to you claim immediate payment of all outstanding charges due to us, terminate or suspend your use of the Services, terminate our relationship with you; or list you with any credit bureau, Internet service provider list, or the South African Fraud Prevention Service. By agreeing to our Terms & Conditions, you expressly consent to this. In all instances, we may retain all Services Fees you have already paid and recover all of our costs associated, including legal costs on an attorney and own client scale (you will be liable to pay our attorneys fees) with your breach.

10.3. Return of hardware or software: Where you have in your possession any of Online Directs hardware or software as a result of using the Service and the related Service ends, you must immediately return the hardware or software to us.

11. Force Majeure

11.1. We will not be responsible for any breach of the Agreement caused by circumstances beyond our control, including fire, earthquake, flood, civil strike, compliance with government orders, failure of any supplier of electricity as well as no electronic communication service etc.

11.2. Survival: Despite termination of the Agreement, any clause, which, from the context, contemplates on-going rights and obligations of the Parties, will survive the termination and continue to be of full force and effect.

12. Acceptable Use Policy

The AUP is a description of the types of activities that are not allowed on Online Directs network and as such forms part of Our Hosting Terms. Online Direct reserves the right to require changes or disable, as necessary, any website, account, database, or other component that does not comply with its established policies, or to make any such modifications in an emergency at its sole discretion. To meet the changing needs of our customers, our business, the Internet environment and the legal landscape, this AUP may be revised at any time and we encourage our customers to review this AUP regularly. If you feel you have discovered a violation of any area of our AUP please report it to abuse@onlinedirect.co.za

SPAM and Unsolicited Email » Online Direct has a zero tolerance SPAM policy.
Server Side Processes » Certain processes are not permitted on our shared systems.
Offensive Content » Certain content is not permitted on Online Directs network.
Internet Abuse » Using our network to engage in illegal, abusive, or irresponsible behaviour is a violation.
Misuse of Account Features » Your account features are for use with your sites only.
Security » Negligence will put Online Directs network at risk.
Shared Systems and Resource Usage » Excessive resource usage will cause performance and stability problems.
Disk Usage » Disk space usage is monitored with automated billing for over-usage.
Traffic Usage » While our traffic usage is generous, it is regulated and is subject to reasonable use.
Combining traffic quotas across multiple servers » It is not possible to combine the traffic quotas of dedicated servers that are combined to deliver a single service.

13. SPAM and Unsolicited Email

Last updated: January 2013.Sending unsolicited commercial communication (including, but not limited to email, instant messaging, SMS, chat rooms, discussion boards and newsgroups) is not permitted via Online Direct's network. Regardless of how the recipient's email address was acquired, if email communication was not explicitly requested or consented to by the recipient or if the recipient would not expect to receive it as a result of an existing relationship, the communication is considered unsolicited (this applies to communication sent to both personal email

addresses and company email addresses e.g. sales@companyxyz.co.za). Email communication that does not clearly originate from a consensual sender or which appears to come from a 3rd party or affiliate is considered unsolicited.

Examples of unsolicited communication:

Purchased mailing lists, "safe lists" and harvesting of email addresses, where the users of those email addresses have not explicitly agreed to receive communication from a specified consensual sender is considered unsolicited. Sending emails where the recipient must opt-out of receiving further emails that they didn't originally request is considered unsolicited. Sending a once-off invitation to receive further information, which was not explicitly requested or consented to by the recipient is considered unsolicited. Email communication to a mailing list including addresses of unwilling recipients or a recipient who has indicated that they wish to be removed from such list, yet continues to receive unwanted emails after a reasonable period, is considered unsolicited.

Mailing list operators should maintain meaningful records of recipient requests and their consent to receive said email communications. There should also be an option for the recipient to unsubscribe from receiving further email communications.

When Online Direct receives a spam complaint, in order to establish if the communication was unsolicited, we may ask you to verify whether the recipient agreed to receive communications from you and if so, when and where you recorded their email address.

Online Direct reserves the right to suspend or terminate the account of any user who sends out unsolicited email otherwise known as Spam with or without notice in accordance with its General Terms and Conditions.

As an Online Direct customer, should you infringe this policy, you will be held liable for any costs incurred by Online Direct, both monetary and in reputation. Online Direct reserves the right to charge the customer of the account used to send any unsolicited email a clean-up fee or any charges incurred for blacklist removal. This cost of the clean-up fee is entirely at the discretion of Online Direct.

The use of any other service for the purposes of sending SPAM with any reference to Online Direct services (including but not limited to mailboxes, autoresponders, and Web pages), will also be grounds for suspension/termination as described above. If your website was compromised and exploited for the purpose of sending unsolicited communications, Online Direct will be more lenient in resolving the issue. However, repeat exploitations of the same website and/or customer account would be grounds for suspension/termination.

14. Offensive Content

14.1. Online Direct does not allow any of the following content or links to such content, to be published on its Hosting Systems:
14.1.1. Content of a pornographic, sexually explicit or violent nature.
14.1.2. "Hate" sites or content that could be reasonably considered as discriminatory in any way including by way of sex, race or age discrimination.
14.1.3. Content of an illegal nature (including stolen copyrighted material).
14.1.4. Content that is defamatory or violates a person's privacy.
14.1.5. Content that involves theft, fraud, drug-trafficking, money laundering or terrorism.
14.1.6. Pirated software sites.
14.1.7. Illegal gambling sites.
14.2. If Online Direct in its sole discretion determines that any customer content violates any law, including the Film and Publications Act, 65 of 1966 or this policy, it may:
14.2.1. Request the customer to immediately remove such content; and/or
14.2.2. Require the customer to modify such content; and/or
14.2.3. Without notice, suspend or terminate access to any services; and/or
14.2.4. Without notice, delete the offending content; and/or
14.2.5. Notify the relevant authorities of the existence of such content (if required by law or otherwise), make any backup, archive or other copies of such material as may be required by such authorities, disclose such elements of the customer's data as may be requested by the authorities and take such further steps as may be required by such authorities.

15. Misuse of account features

15.1. Operating any service which makes an account feature available to third parties for any use other than normal access to that account's Web site is forbidden. Operating any service which enables or assists anonymous or abusive behaviour by third parties is forbidden. Operating any service which affects the stability or reliability of any Online Direct server or network component, impacts other users or the company negatively, or degrades quality of service is forbidden. All account features are to be used solely in order to develop and implement the Web site(s) associated with that account.
15.2. Reselling Multiple Domains on Online Direct's Web Hosting packages to a third party is not allowed. Multiple Domains are to be used solely for the Profile Owner's own websites.

16. Shared Systems and Resource Usage

16.1 Last updated: August 2012. Customers hosting on our shared environment may not use any shared system provided by Online Direct in a way that interferes with the normal operation of the shared system, or that consumes a disproportionate share of the system's resources. For example, excessive server hits, excessive bandwidth usage, excessive disk usage, inefficient scripts or database queries may compromise other users of the shared hosting environment. Online Direct is authorised to suspend a user's account should it be found that excessive resource usage is negatively impacting on other customers of our shared hosting environment. In most cases, the examples below do not apply to Online Direct Dedicated servers.

16.2 Users may not, through a cron job, CGI script, interactive command, or any other means, initiate the following on Online Direct's shared servers:

16.2.1 Run any process that requires more than 50MB of memory space.
16.2.2 Run any program that requires more than 30 CPU seconds.
16.2.3 Run more than 10 simultaneous processes.
16.2.4 Send out mail to more than 500 recipients (email addresses) within one hour. 500 recipients represent one of the following: 500 recipients for one email, 500 individual emails or a combination of the two.
16.2.5 Send or receive, through mail, any file larger than 20MB.
16.2.6 Should we discover that a customer is performing bulk mail runs on our shared systems that exceeds the limit communicated in 4.1.4 above, regardless of whether it constitutes SPAM or not, Online Direct will deactivate the user's account.
16.2.7 Custom server-side CGI scripts are to be run only by users with the appropriate package types (in Online Direct's case the Web Hosting Basic package or higher). No user may run CGI scripts for the benefit of external sites or services. The use of system resource limits is intended to prevent runaway CGI scripts on an unattended server. Also, processes with large memory footprints or hungry CPU requirements will incur swapping and other slowdowns that cause problems for every site on the server
16.2.8 Interactive Web applications, commonly known as "chat", are not allowed on Online Direct's shared systems. These applications are better placed on dedicated servers.
16.2.9 MySQL databases are provided to users of the Web Hosting Basic package and higher:
16.2.10 Each qualifying individual package is limited to the allocated quota as published in the product matrix.
16.2.11 Each individual database is allotted a maximum of 500 MB disk space.
16.2.12 Databases may not be used for circumventing package disk allowances by storing web sites within the database.
16.2.13 Databases may only be used in conjunction with Online Direct hosted packages. Access to databases from outside our local network is provided strictly for site and database development.
16.2.14 Only 10 concurrent MySQL connections per database user are allowed.
16.2.15 Databases may not be used to store binary files (including but not limited to image and application files). The database needs to reference the image on the user's site rather than actually storing the image i.e. these files should be stored within the user account and referred to in the database by using a link.
16.2.16 Online Direct reserves the right to require changes to databases and database usage should they have an adverse impact on a database server and/or other user databases on that server. Online Direct may move the database to a new server, or in extreme cases, Online Direct reserves the right to disable any database determined to be harming performance of a database server.
16.2.17 The use of "cron jobs" (processes that are run automatically at certain times, in accordance with a "crontab" file set up by each user), are allowed on Online Direct servers, subject to the following conditions and restrictions:
16.2.18 To be used only by customers of the Web Hosting Basic package and higher.
16.2.19 The job must not execute more often than every two hours.
16.2.20 If a cron job is likely to consume excessive CPU usage, it should be given a lower CPU priority.
16.2.21 Resource limits are enforced by automatic monitoring systems. This is not applicable to Fully Managed Dedicated servers, providing that it does not interfere with Online Direct's ability to manage the server on the customer's behalf.

17. Server side processes

17.1 The installation or operation of any stand-alone, unattended server-side process (daemons) on Online Direct servers, with the exception of cron jobs is not possible. Violation of this policy will result in immediate account termination without warning. This is not applicable to Online Direct's dedicated servers, providing that it does not interfere with Online Direct's ability to manage the server on the customer's behalf.
17.2 This policy exists for several reasons:
17.3 To protect the CPU and memory resources available on each server.
17.4 To protect and enhance system security by not allowing unapproved third-party programs to accept connections from the outside world.

18. Internet Abuse

18.1. Unauthorised access to or use of data, services, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to break security or authentication measures without express authorisation of the owner of the system or network;
18.2. Monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;
18.3. Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
18.4. Use of an Internet account or computer without the owner's authorisation;

18.5. Collecting information by deceit, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;
18.6. Use of Online Direct's service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
18.7. Any activity or conduct that is likely to result in retaliation against our network;
18.8. Any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including the Electronic Communications and Transactions Act 25 of 2002 (see ECT Act) which renders you liable to a fine or imprisonment;
18.9. Introducing intentionally or knowingly into Online Direct's service any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Web;
18.10. Forging email or other messages is forbidden. Trafficking in pirated software is forbidden. Port scanning or the use of similar tools is forbidden.
18.11. Use of Online Direct services to publish or otherwise disseminate information about the availability of pirated software or other material that is being made available illegally, including the publication of a list of links to such material, regardless of disclaimers, is specifically forbidden. We do not condone any illegal material or behaviour.
18.12. Compliance with the acceptable use policies of any network or system with which you connect through our service is required. If inappropriate activity is detected, all accounts of the user in question will be deactivated until the investigation is complete. Prior notification to the user is not assured. In extreme cases, law enforcement will be contacted regarding the activity

19. Security

19.1 Online Direct customers must take reasonable security precautions. Negligence could result in the hacking of websites as well as compromised mailboxes due to vulnerable PCs, website software or the use of weak passwords, which could affect other Online Direct customers through blacklisting, phishing or spamming.
19.2 It is the customer's responsibility to ensure that scripts/programs installed under their account are secure (using the latest version) and permissions of directories are set properly, regardless of installation method. Users are ultimately responsible for all actions taken under their account. This includes the compromise of credentials such as user name and password. It is required that customers use a secure password. If a password is found to be weak, Online Direct will notify the user and allow time for the user to change/update the password. Failure to make a password change that inadvertently leads to the website being compromised could result in the user's account being suspended / terminated.
19.3 Passwords should consist of at least 11 mixed alpha and numeric characters with case variations. Customers should not use a common word as a password and should change their passwords regularly. In the event of abuse Online Direct reserves the right to reset a password.

20. Disk usage

20.1. Accounts with many files can have an adverse effect on server performance. Online Direct has the following limit: 200 000 files (i.e. an email, webpage, image file, folder etc.), or 50 000 files per folder. Accounts exceeding the above limit will have those files and/or folders excluded from our backup system.
20.2. Using our servers as a personal storage facility is not permitted. Any content stored must be directly related to the website(s) in question.
20.3. Mailboxes that build up large volumes of email without being accessed are not allowed (e.g. catchall mailboxes or bounce message mailboxes). The primary cause of excessive disk usage can be due to customers having their catchall address enabled, yet never checking their primary account mailbox. Over time, tens of thousands of messages build up, pushing the account past our file limit.
20.4. Email older than five years may not be stored on the server.
20.5. Individual emails that are 5 MB or larger may not be stored on the server for more than 1 month.
20.6. Online Direct has a disk usage quota in place for its Web Hosting packages. Where applicable, customers are sent monthly emails from Online Direct notifying them of domains that have exceeded the allocated quota, providing an opportunity to reduce disk space or upgrade to a higher package in order to avoid unnecessary charges for over-usage. Customers can regularly monitor their disk usage via konsoleH by clicking on 'Disk Usage' under Statistics & Reports, which will give customers a reading of the total size of the package together with a summary of individual folder sizes.
20.7. In order for Online Direct to operate with greater efficiencies and for our customers to have the flexibility and control of actively managing their disk space, an automated system tracks, notifies and charges for over-usage.

21. Traffic Usage

21.1. Our Web Hosting packages do not have a set quota on the data transfer (traffic) provided as we'd like our customers to have the resources needed to offer a viable, growing online presence. Find out more about our **unlimited traffic policy** section 23 below. It is expected that all customers comply with this Acceptable Use Policy, designed to preserve Online Direct's server and network performance for the benefit of all our customers.
21.2. Using our Web Hosting packages primarily for online file storage, archiving electronic files or streaming excessive video or hosting music is not permitted.

21.3. Certain services may not be hosted on our dedicated servers & our Colocation offering without prior consultation. Examples include, but are not limited to:
21.3.1. Public mirroring services that are made available for general public use
21.3.2. Any website or service where the primary focus is to drive or redirect traffic from one network to another
21.3.3. Reselling bandwidth and/or network capacity as internet access to end users If you'd like to discuss your requirement in more detail, please contact sales@Onlinedirect.co.za

22. Combining traffic quotas across multiple servers is not supported

First, the general principle regarding quotas: The generous quotas provided by hosting providers are based on an aggregated usage model. What this means is that each hosting product, at full quota use, runs at a loss. In reality, 99% of customers use a fraction of their quotas while less than 1% are high or excessive users. As a result, the aggregate usage across the cumulative customer base remains within profitable margins. This makes it entirely feasible to offer quota levels that provides both peace of mind as well as the flexibility for occasional or permanent high usage without raising the cost. Regarding combined dedicated server traffic quotas: In the case of dedicated servers (Managed Dedicated & TruServ) that are combined to deliver a single service, the principle of an aggregated usage model cannot be applied. When lumped together to service an ever growing need, it is as though a "super-computer" is being created and the traffic quotas that are allocated to its parts are not subject to an aggregated usage model. In other words, it's a new product with different product characteristics. Traffic routed between Colocation Racks and TruServ Servers: Traffic generated from a Colocation network that is destined for the internet should not be routed via a TruServ server or network. **Examples:** An example would be the hosting of a video processing system which requires a large number of servers to perform the required processing, including database, backup and redundancy servers. Combining the quotas of all the servers used for this purpose into a single large quota is simply not feasible due to the loss that this would incur for Online Direct. **Other examples are:** Very popular Websites (eg. news24.com) Large SaaS implementations Servers used for mass download purposes or caching proxies Mass mail services (eg. a free Webmail service) Shared hosting Cloud hosting platforms **What now?** 99% of customers with clustered servers remain well within the acceptable aggregated data usage pattern. A further 1% may be contacted to discuss a viable quota model. So why do we explain this policy so elaborately? Because we want you to understand the basis on which you are using the service and to give us the recourse to collaborate with you on options should we feel the need to do so. Very simply, if you are not being contacted, it's not a concern for us. If you are concerned or would like greater predictability, please sales@onlinedirect.co.za

23. Unlimited Traffic Policy

What does unlimited mean? Unlimited means that Online Direct does not impose a quota limit. **Traffic is no longer the first point of constraint in shared hosting.** A fraction of websites have always generated the vast majority of traffic. The use of quotas capped the risk of pushing aggregate traffic consumption beyond a viable threshold. However, traffic costs have persistently declined over time, to the extent that they can be regarded as no longer being the first point of constraint. The server hardware infrastructure has now assumed that role. The term 'shared hosting' implies that a server is shared by multiple customers. Online Direct's powerful servers are typically underutilised with their low ratio of sites per server. This allows websites to grow and spike without compromising performance. 99% of websites will exist in this dynamic environment. **How will I know that my site is unsuited to a shared hosting server?** Simply, if one site singularly compromises shared server performance it has outgrown that environment. Less than 1% of sites are affected. Determining that threshold upfront is difficult. We actively monitor server performance and will contact a site owner if necessary to discuss alternatives. Causes range from coding (in) efficiencies, poor security maintenance practices and high demand or a combination. Where no gains in efficiency can be made, a dedicated server is the natural outcome. It is also important to observe our Acceptable Use Policy (AUP). **What happens to my site if it is deemed unsuitable for shared hosting?** We will contact you proactively to discuss a suitable course of action and implementation timeframe. In an emergency, our priority is to protect the integrity of the server for all other, legitimate users. In that case we may temporarily suspend your site, but will be equally pressed to ensure that your services are re-instated as swiftly as reasonably possible.