The Acceptable Use Policy is a description of the types of activities that are not allowed on our network and as such forms part of Our Hosting Terms.

DC Integrated Solutions 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@dcis.co.za.

1. 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 our 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.

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

- When DC Integrated Solutions 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.

- DC Integrated Solutions 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 a DC Integrated Solutions customer, should you infringe this policy, you will be held liable for any costs incurred by DC Integrated Solutions, both monetary and in reputation. DC Integrated Solutions 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 DC Integrated Solutions.

- The use of any other service for the purposes of sending SPAM with any reference to DC Integrated Solutions 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, DC Integrated Solutions 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.

- **What are the industry best practices regarding SPAM? Which should I follow?**

  In order to prevent being labeled a spammer, you need to ensure that your intended recipients have given their consent to receiving an email via some affirmative means, such as a double opt-in procedure.

It is also important that you have procedures in place that would allow the recipient to easily revoke their consent i.e. an 'unsubscribe' or 'remove' link in the mail.

Best Practices to conduct a legitimate mailing list includes:

- Make use of a double opt-in procedure. Not only must the user take action to add himself to a list, but he then receives a confirmation email of his subscription. He must reply to the email to be added to the list. This is done to ensure that the customer did not subscribe by mistake or somebody else did not subscribe him to receive your regular email.
- A 'remove' or 'unsubscribe' link (an opt-out procedure) must be provided to make it easier for the recipient to revoke consent or to terminate their subscription. Mailings must cease promptly once a subscription is terminated.
- Mailing list administrators must take adequate steps to ensure that their lists are not used for abusive purposes.
- Avoid multiple font sizes and colours as these promote mail being flagged as spam.
- Blank spaces increase your spam percentage allocated by most scoring systems.

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

2. Offensive Content

Last updated: May 2011.

1. DC Integrated Solutions does not allow any of the following content or links to such content, to be published on its Hosting Systems:
    1. Content of a pornographic, sexually explicit or violent nature.
    2. "Hate" sites or content that could be reasonably considered as discriminatory in any way including by way of sex, race or age discrimination.
    3. Content of an illegal nature (including stolen copyrighted material).
    4. Content that is defamatory or violates a person's privacy.
    5. Content that involves theft, fraud, drug-trafficking, money laundering or terrorism.
    6. Pirated software sites.
    7. Illegal gambling sites.

2. If DC Integrated Solutions 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:
    1. Request the customer to immediately remove such content; and/or
    2. Require the customer to modify such content; and/or
    3. Without notice, suspend or terminate access to any services; and/or
    4. Without notice, delete the offending content; and/or
    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.

3. Misuse of account features

Last updated: July 2011.

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 DC Integrated Solutions 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.
2. Reselling Multiple Domains on DC Integrated Solutions'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.

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

4. Shared Systems and Resource Usage

Last updated: August 2012.

Customers hosting on our shared environment may not use any shared system provided by DC Integrated Solutions 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. DC Integrated Solutions 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 DC Integrated Solutions Dedicated servers.

1. Users may not, through a cron job, CGI script, interactive command, or any other means, initiate the following on DC Integrated Solutions's shared servers:
    1. Run any process that requires more than 50MB of memory space.
    2. Run any program that requires more than 30 CPU seconds.
    3. Run more than 10 simultaneous processes.
    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.
    5. Send or receive, through mail, any file larger than 20MB.

2. 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, DC Integrated Solutions will deactivate the user's account.
3. Custom server-side CGI scripts are to be run only by users with the appropriate package types (in DC Integrated Solutions'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.
4. Interactive Web applications, commonly known as "chat", are not allowed on DC Integrated Solutions's shared systems. These applications are better placed on dedicated servers.
5. MySQL databases are provided to users of the Web Hosting Basic package and higher:
    1. Each qualifying individual package is limited to the allocated quota as published in the product matrix.
    2. Each individual database is allotted a maximum of 500 MB disk space.
    3. Databases may not be used for circumventing package disk allowances by storing web sites within the database.
    4. Databases may only be used in conjunction with DC Integrated Solutions hosted packages. Access to databases from outside our local network is provided strictly for site and database development.
    5. Only 10 concurrent MySQL connections per database user are allowed.

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

6. 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.
7. DC Integrated Solutions 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. DC Integrated Solutions may move the database to a new server, or in extreme cases, DC Integrated Solutions reserves the right to disable any database determined to be harming performance of a database server.

6. 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 DC Integrated Solutions servers, subject to the following conditions and restrictions:
    1. To be used only by customers of the Web Hosting Basic package and higher.
    2. The job must not execute more often than every two hours.
    3. If a cron job is likely to consume excessive CPU usage, it should be given a lower CPU priority.
7. Resource limits are enforced by automatic monitoring systems. This is not applicable to Fully Managed Dedicated servers, providing that it does not interfere with DC Integrated Solution's ability to manage the server on the customer's behalf.

5. Server side processes

Last updated: May 2011.

1. The installation or operation of any stand-alone, unattended server-side process (daemons) on DC Integrated Solutions servers, with the exception of cron jobs as per point 4 above, is not possible. Violation of this policy will result in immediate account termination without warning. This is not applicable to DC Integrated Solutions's Dedicated servers, providing that it does not interfere with DC Integrated Solutions's ability to manage the server on the customer's behalf.
2. This policy exists for several reasons:
    1. To protect the CPU and memory resources available on each server.
    2. To protect and enhance system security by not allowing unapproved third-party programs to accept connections from the outside world.

6. Internet Abuse

Last updated: May 2011.

You may not use our network to engage in illegal, abusive, or irresponsible behaviour, including:

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

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

security or authentication measures without express authorisation of the owner of the system or network;
2. Monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;
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;
4. Use of an Internet account or computer without the owner's authorisation;
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;
6. Use of DC Integrated Solutions's service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
7. Any activity or conduct that is likely to result in retaliation against our network;
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;
9. Introducing intentionally or knowingly into DC Integrated Solutions'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;
10. Forging email or other messages is forbidden. Trafficking in pirated software is forbidden. Port scanning or the use of similar tools is forbidden.
11. Use of DC Integrated Solutions 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.

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.

7. Security

Last updated: May 2011.

DC Integrated Solutions 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 DC Integrated Solutions customers through blacklisting, phishing or spamming.

1. 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, DC Integrated Solutions will notify the user and allow time for the user to change/update the password. Failure to make a

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

password change that inadvertently leads to the website being compromised could result in the user's account being suspended / terminated.

2. 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 DC Integrated Solutions reserves the right to reset a password.

For further information, please read our FAQ on Secure Passwords.

8. Disk usage

Last updated: May 2011.

1. Accounts with many files can have an adverse effect on server performance. DC Integrated Solutions has the following limit: 100 000 files (i.e. an email, webpage, image file, folder etc.), or 25 000 files per folder. Accounts exceeding the above limit will have those files and/or folders excluded from our backup system.
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.
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.
4. Email older than five years may not be stored on the server.
5. Individual emails that are 5MB or larger may not be stored on the server for more than 1 month.
6. DC Integrated Solutions has a disk usage quota in place for its Web Hosting packages. Where applicable, customers are sent monthly emails from DC Integrated Solutions 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.
7. In order for DC Integrated Solutions 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.

9. Web Hosting Traffic Usage

Last updated: March 2014.

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. However, it is expected that all customers comply with this Acceptable Use Policy, designed to preserve DC Integrated Solutions's server and network performance for the benefit of all our customers. Our Web Hosting

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

packages are not suited to support the sustained demand of large enterprises; in such cases a dedicated server would be more appropriate.

2. Using a Web Hosting package primarily for online file storage or archiving electronic files is not permitted.
3. Streaming excessive video or hosting music on a Web Hosting package is prohibited.

10. Combining traffic quotas across multiple servers is not supported

Last updated: September 2014.

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 can not 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 DC Integrated Solutions.

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

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za

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 contact support@dcis.co.za.

integrated solutions
DC Integrated Solutions
079 030 1539
info@dcis.co.za
www.dcis.co.za