

Dynamic Servers Limited – Resources Usage Policy

1. Background

- 1.1. The purpose of this policy is to define a fair use of shared resources on our web hosting network. We believe that our clients are entitled to a fair usage of our services. Each user has pre-set of allocated resources for their hosting environment.
- 1.2. This policy outlines those allocations. It also outlines what is not permitted on our services. We are committed to providing our clients with a top-quality service. We hope that this policy will filter out the bad practices from our hosting networks.

2. Resource Usage Limits

- 2.1. Each Individual cPanel account that is created has its own resource limits. The majority of users will not reach these limits.
- 2.2. Each cPanel account has been allocated with the following: 1CPU core, 0.5GB Ram 4MB/s of I/O, 20 PHP Processes, 30 Concurrent SQL Connections*, 60 Total Processes, 250,000 Files, 0.5GB Max DB Size.

2.3. Databases

- 2.3.1. Accounts should not exceed an average of 1 second of CPU time per query for MySQL queries performed in any given hour.
- 2.3.2. Databases may not be accessed by externally hosted sites, except for the purpose of administering the database.
- 2.3.3. Databases may not be shared between accounts
- 2.3.4. *The default concurrent MySQL connection limit is 30.

2.4. Emails

- 2.4.1. Attachments larger than 25MB in size must not be sent by email.
- 2.4.2. IMAP/POP Email Boxes have a maximum size of 4GB each. Old mail must be archived or deleted to remain below this limit.
- 2.4.3. Outbound emails should not be sent to more than 50 recipients at any one time. If an email needs to be sent to more than 50 recipients, then a form of mailing list software should be used.

- 2.4.4. Mailing lists / email marketing emails can be sent to a maximum of 2,000 unique recipients.
- 2.4.5. Any emails sent to a mailing list must contain an unsubscribe link to an automated removal system. This system should not be password protected.
- 2.4.6. No more than 200 emails may be sent per hour.

2.5. Processes – Any process that are attributed to or initiated by your user account, must not:

- 2.5.1. Create core dump files.
- 2.5.2. Execute a script or binary that forks in a way to create a fork bomb, spawn subprocesses.
- 2.5.3. Run in the background.
- 2.5.4. Listen to a network port.
- 2.5.5. Open more than 100 files.
- 2.5.6. Open or access a file greater than 2GB size.

2.6. Shell Access

- 2.6.1. You're are not permitted to log into any other server or network from our servers.
- 2.6.2. You may not use the "find" command recursively on folders that are more than five levels deep.

2.7. Unsolicited Email / SPAM

- 2.7.1. We do not permit emails to be sent from "brought lists". Emails must only be sent from lists that you have collected yourself.
- 2.7.2. If you violate this policy, your account will be subject to investigation and may be terminated without notice. Any damages will be prosecuted to the full extent of the law.

2.8. Content Restrictions

2.8.1. Adult Content

- 2.8.1.1. We do not permit any pornography, including adult oriented pictures, videos, links to adult sites or sites containing content of a sexually explicit nature.

2.8.2. Backups, Storage Archives & FTP Storage Space

2.8.2.1. Hosting accounts are only to be used for the purposes of hosting web sites and emails. They are not to be used to back up content from remote computers, as a general file storage system or as an FTP upload repository. One backup of your account is permitted to be stored within your space. These must not be stored for more than 45 days. The storage of audio music, videos, photos or other downloadable media, unless these files are being used specifically on your publicly accessible web site.

2.8.3. Trash Box

2.8.3.1. cPanel operates a “trash box” system. This allows you to restore files which were deleted from the File Manager or recover emails which have been added to the IMAP trash box. All files and emails in the “trash box” will count towards your total disk space usage.

2.8.4. Chat Software

2.8.4.1. We do not permit real time chat software to be hosted from within your hosting account. Third party chat solutions that integrate with your website but are remotely hosted are permitted.

2.8.5. We Applications

2.8.5.1. All third-party web applications that you install must be kept up to date. Failure to keep third part applications up to date can lead to security vulnerabilities, this can lead to the server being exploited. It is your responsibility to regularly check for application updates. We would recommend checking at least twice a month. Any applications which are being exploited will be quarantined automatically. We will contact you to advise you of the situation.

2.8.6. General

2.8.6.1. The following are strictly prohibited:

2.8.6.1.1. Banner rotation services & link exchanges. Bit torrent or other peer-to-peer applications, trackers and clients. Offering of free or paid image, file, document or data storage. Offering free hosting or email services. Online RPGs, hate sites, sites that promote hacking, SPAM, warez content or other illegal activities. Material that infringes

any rights (including Intellectual Property Rights) of any third party.
Operating a public download mirror. Running a gaming server.
Running a proxy server or anonymizer, either publicly accessible or password protected. Web spiders and indexers. IRC Egg Drops & Related Programs. UltimateBBS, Ikonboard, YaBB, YabbSE. Shell, SSH, Telnet Scripts and all alternatives. formmail.pl, formmail.php, formmail.cgi OR alternative names for the same script, except the secure version available for install from the Control Panel. Any script using a large flat file database.