



Bizo Email Filter

Service Description



Copyright © 2004 Business Online Limited

Bizo is the trading name for Business Online Limited. This document is free to view in electronic form via your World Wide Web browser, however Bizo maintains copyright. You are entitled to make one copy for research purposes, however you may not further copy or republish them or store them in your computer or elsewhere except as required by your browser for the sole purpose of viewing them while using the browser.

This document is the property of Business Online Limited (Bizo) and is made available only upon these terms and conditions. Bizo reserves all rights herein. Reproduction or disclosure other than under these terms in whole or part is permitted only with the written and express consent of Bizo.

All liability of any nature whatsoever in relation to the information contained in this report is excluded.

All rights are reserved.

Document Reference Information

Authors / Group	Business Online Ltd
Release Date	7 th November 2006
Revision	Version 1.1 Released: 1-11-2004 Version 2.0 Released: 7-08-2006 Publish Draft

TABLE OF CONTENTS

1.	What is Bizo Email Filter	6
2.	What are the benefits of Bizo Email Filter?	7
3.	How does Bizo Email Filter work?	9
3.1	Service Description	9
3.1.1	Bizo Mail Relay Service	10
3.2	What's Included.....	10
3.3	Domain Names and MX Records	10
3.4	Challenge Response Mechanism	11
3.5	CatchAll Filter	11
3.6	Heuristic Antivirus Technology	11
3.7	Dynamic Outbreak Management.....	11
3.8	Filter Language Independence.....	12
3.9	Whitelists and Blacklists	12
3.10	Remote Access Quarantine	13
3.11	Web-Based Statistics and Management Reporting	13
3.12	Adding new Users.....	13
3.13	Notifications.....	13
3.14	Advanced Custom Settings.....	13
3.15	High Availability Features	14



3.16	Virus Rules.....	14
3.17	Virus Signature Updates.....	14
3.18	Notification Rules.....	15
3.19	All Standard Mail Formats Supported.....	15
3.20	Ongoing System Supervision and Performance Monitoring	15
3.21	User Self-Management.....	15
3.22	Anti-Porn Filter	17
3.23	Customer Administrator and User Guides	17
3.24	Content Policy Management.....	17
3.25	Content Filtering.....	17
3.26	Bizo Email Filter Summary.....	18
3.27	Integration with other Bizo services.....	19
3.27.1	Get Connected.....	19
3.27.2	Get Secure.....	19
3.27.3	Get Working.....	20
3.27.4	Get Talking.....	20
3.28	Quality Assurance and Change Management.....	20
3.29	Ongoing System Supervision and Performance Monitoring	21
4.	Is Bizo Email Filter for you?.....	22
5.	What are Your Responsibilities?	23
5.1	Bizo Service Offer and Terms.....	23
5.2	Unique Mail Domain	23
5.3	Acceptable Use Policy.....	23



5.4	Privacy Policy.....	23
5.5	Support.....	23
5.6	Feedback.....	24
6.	Installing Bizo Email Filter.....	24
7.	Online Configuration of Bizo Email Filter.....	24
8.	On-line Reporting.....	24
9.	Copyright Information.....	25

1. What is Bizo Email Filter

Email is now one of the most important business tools. Businesses rely on email for cost-effective communication with customers, suppliers, partners and their employees. More and more time is lost each day as staff sort through their daily email SPAM messages. New and more deadly viruses are released everyday. The impact of undetected viruses on an in-house email system can put you out of action with disastrous consequences.

A small business can't usually justify the cost of having technical expertise on-hand to implement new anti-virus and SPAM defenses as they are released, however the risk of ignoring the problem is also unacceptable.

Bizo Email Filter is a simple but effective solution that works in the background to ensure your company and staff are not impacted by malicious, unsolicited and unsavoury emails and virus attacks. Bizo Email Filter is the complete solution – anti-spam, anti-virus, anti-porn, and content management. Bizo Email Filter protects your data and enhances the efficiency of email as a communications medium.

With Bizo Email Filter you do not have to buy, install or maintain software on any servers, desktops or laptop PCs in your organisation. Bizo Email Filter is a simple subscription service, and once activated for an email domain, all email – inbound and outbound – passes through the Bizo Email Filter engine before it reaches it's destination.

The Bizo Email Filter has a number of key advantages:

- It operates at the Internet level – intercepted spam and viruses never reach your network
- It can be applied to any email domain – it does not matter which ISP you use
- It traps up to 99% of spam with no wanted emails lost
- Continuous automatic updates are applied for known virus signatures
- Heuristic analysis traps new viruses and worms
- Bizo Self Service Portal provides configuration and quarantine management through web-based front end.
- Bizo Self Service Portal provides enhanced Statistics and Reporting by Web browser
- 24 hour Technical Centre supervision, support and response to virus alerts

2. What are the benefits of Bizo Email Filter?

Many businesses are realising that in-house technology is becoming more and more distracting and expensive. Bizo Email Filter allows you to continue to maintain your in-house email system without having to invest in the hardware, software and technical expertise and time to implement, manage, maintain and upgrade you own email security system.

Bizo Email Filter is a fully outsourced service that gives you a complete and specialist service with no capital outlay or technical skills required. The benefits of using Bizo Email Filter for scanning your email include:

- No software or hardware to deploy or manage
- No capital investment
- Low-cost pre-defined monthly charge with no hidden or unexpected support, maintenance or upgrade costs.
- Service maintained by 24/7 specialists
- Stay leading-edge with updates and technology
- Release expert resources from routine tasks
- Free up network resources and access bandwidth
- No ongoing administration overheads
- Provides an advanced level of email security for your in-house email system
- Policy-based control of email usage, SPAM and viruses
- Includes easy access to online reports showing usage detail and security infringements
- Maintained with current anti-virus signatures and malicious attack defense patches
- Includes online self service functions
- Enforces your Email Acceptable Usage Policy
- Easily Scalable – your subscriber base can grow with no hardware or software investment required.



- Easy to Use - intuitive, user-friendly interface; administrator access to timely, live technical support.
- Predictable Monthly Cost – Each month you know exactly what your email will cost. You will have no emergency new equipment bills or huge excess data charges.
- Stay in Charge – Your staff administrators can control every aspect of managing your email policy and reporting.
- No Technical Expertise Required – Bizo provides email services for many businesses. We have built an enterprise-level infrastructure that most companies cannot afford to invest in. Bizo Email Filter is delivered with a quality of service that few organizations can enjoy:
 - Our services are monitored 24 hours a day, every day.
 - We keep spare parts on hand for rapid replacement in case of hardware issues.
 - All software updates and security patches are thoroughly tested in our testing environment before production deployment.
 - Automated Intrusion detection systems are active day and night to ease your worries.
 - The Bizo Self Service Portal offers a sophisticated web-based interface to ease administration, without risk.

3. How does Bizo Email Filter work?

Bizo Email Filter is based on the integration of Anti-spam Agents, Multiple Antivirus Scanners, and the Cortex™ automated provisioning and reporting platform.

Every email transiting through Bizo Email Filter service is processed by a chain of separate anti-virus scanners. The first are generally commercial scanners. The final scanner is a heuristic proprietary email filter engine. At each stage, when a scanner detects a virus, the email concerned is removed from the message flow and deposited in a 'quarantine' storage area.

Bizo Email Filter also runs anti-spam processing on all emails through the system. The service uses multiple anti-spam technologies including global black lists, customer defined black and white lists per email domain, and individual self-managed black and white lists for each email address.

Bizo Email Filter incorporates a wide range of heuristic tests on mail headers and body text to identify spam. The spam scoring thresholds used are under configuration control by the customer administrator, who can choose the criteria against which potential spam is dropped (from quarantine after a pre-set safety delay) or deposited in a spam quarantine store for later examination and deletion. Customer email administrators can also easily manage the domain-based white lists, black lists and quarantined emails via the secure web management interface.

Customer email administrators can also define domain-specific email scanning criteria including:

- Turn on or off inbound and/or outbound spam and anti-virus scanning.
- Turn on or off inbound and/or outbound footers.
- Denial of specific attachment types.

3.1 Service Description

Bizo Email Filter . Available features are summarised in the following table.

Components	Included within Bizo Email Filter
Multiple Antivirus Engines	YES
Fully Managed Service	YES
Customer managed domain-based rules	YES
User Configurable Antispam	YES
User Managed White & Blacklists	YES
Web-based Management Tool	YES
Heuristic Antivirus	YES

Catch-all Facility	YES
Outbound Mail Security	YES
Reports and Statistics	YES

Please note that the Bizo Email Filter service is included, by default, for all subscribers to BizoMail services. Bizo Email Filter however can easily be applied to email provided by your in-house IT department, or other 3rd party national and international email service providers.

3.1.1 Bizo Mail Relay Service

Bizo Email Filter is also available as a simple Email Relay service. In this case no emails are scanned and no domain or user-based management is configured. This service is available without additional fee for Bizo customers subscribing to Bizo Network services.

3.2 What's Included

Bizo Email Filter includes:

- 30-Day Free Trial.
- Service Activation.
- Support.
- 24 x 7 system monitoring, maintenance and upgrades.
- Bizo Email Filter website access to Email Policy Administration, Quarantine and Online Reports.
- No onsite software or hardware required.

3.3 Domain Names and MX Records

We recommend that, if you don't already own a unique domain name for your business, that you subscribe to one. We can assist you to arrange this. The benefit to you is that it remains yours, that you are in control of it and that it is portable.

Once this is arranged we will configure an MX Record within the Bizo Email Filter environment to ensure email is routed through the scanning service to your staff and customers.

While Bizo Email Filter is included by default with all Bizomail email accounts it can also be easily configured for either in-house email systems or 3rd party hosted email providers.

3.4 Challenge Response Mechanism

Bizo Email Filter uses a unique technology that notifies a sender if a message is caught as spam, and allows him to release the message from quarantine for delivery to the intended (Bizo Email Filter user) recipient. This is achieved without any action by the user.

This system effectively guarantees that if a genuine (i.e. not a spammer) wants to send an email to a Bizo Email Filter user, the message WILL be delivered – regardless of how aggressive the antis spam filter is set.

In other words, using Bizo Email Filter it is possible to reach the near-ideal spam filter characteristics – almost 100% of spam stopped and NO GOOD EMAILS LOST.

Each day every email user receives a Bizo Email Filter Quarantine report showing quarantined emails. It is easy to check each email and either delete or release them. Quarantined emails are retained for 30 days.

3.5 CatchAll Filter

A common spamming technique is to email random email addresses for a domain and, on the basis of automatic replies, build a database of valid email addresses (called directory harvesting). This has made it hard for email administrators to both defend against directory harvesting and track genuine emails sent to incorrectly addressed accounts.

Bizo Email Filter allows you to both defend against directory harvesting and track incorrectly addressed emails.

All emails sent to your domain that do not have an authenticated address are quarantined and no automatic replies are forwarded to the sender. The domain email administrator can release or delete the quarantined emails.

3.6 Heuristic Antivirus Technology

Bizo Email Filter heuristic anti-virus engine has the ability to trap new viruses and worms from the very outset, even before signatures have been released from the traditional anti-virus vendors. This technology does not use signatures, but an extensive knowledgebase of virus and malware techniques and methods which can be identified by analysis during the scanning process.

3.7 Dynamic Outbreak Management

In addition to robust heuristic technology, Bizo Email Filter offers Dynamic Outbreak Management, as a feature of the managed service. Most worm outbreaks are spread by emails that have easily identified characteristics, and the outbreak can therefore be stopped

dynamically, by email signature, many hours before an actual virus signature is available from traditional anti-virus vendors.

3.8 Filter Language Independence

Bizo Email Filter has the capability to be truly language independent. Our leading-edge Bayesian filtering technology is SELF-LEARNING in any language, including non-latin and double-byte character sets – including Chinese (traditional AND simplified), Thai, Russian, Korean, etc. For example, in independent tests, this system was proved to perform far better than competitive systems in identifying Chinese language spam.

3.9 Whitelists and Blacklists

White and Black lists can be managed by the domain administrator on behalf of the whole domain or by the user for their own email address. Note that the domain administrator cannot manage an individual user's white and black lists.

A White List is a list of people who send email that should never be marked as spam. It is recommended to include automated addresses on this list as well. For example, if a bank sends a statement via email, include the address from which the bank sends out email on the whitelist. Wildcards can be used on this list (i.e. [fred*@somedomain.com](#) or [*@*.somedomain.com](#), or [*@somedomain.com](#)).

A Black List is a list of addresses from which email is never desired. Email from any address on this list is always marked as spam. Wildcards can be used on this list (i.e. [*@somedomain.com](#), [fred*@somedomain.com](#) or [*@*.somedomain.com](#)).

Users and email domain administrators can also configure their Spam Eliminating rules. This setting controls how much spam is quarantined in addition to being tagged. The following Spam Eliminating settings are available:

- None, No spam is eliminated from email
- Conservative, Only the most obvious spam is eliminated. Users may still receive a lot of spam.
- Moderate, A lot of spam is eliminated. Users may still receive some spam.
- Aggressive, Nearly all spam is eliminated. It is possible that a legitimate email may be eliminated if it looks too much like spam.

3.10 Remote Access Quarantine

The secure web-based quarantine ensures users can log in, using their standard email address and password anywhere in the world to release or delete their quarantined emails.

3.11 Web-Based Statistics and Management Reporting

The customer email administrator is given secure access to the Bizo Email Filter website from where you can manage all configurable features of the Bizo Email Filter service, and generate reports and statistics relating to virus incidents, spam and general email usage and volume per user account.

3.12 Adding new Users

As Bizo Email Filter is domain-based once a new email account is created it is automatically included within the email domain's spam and anti-virus scanning rules.

3.13 Notifications

Whenever the system detects and quarantines a virus-suspect email, a response message can automatically be sent to the sender of the email, and an email alert is sent to the customer administrator.

For normal emails passing through the system, a brief footer is appended explaining that each email has been scanned by Bizo Email Filter and is spam and virus-free.

3.14 Advanced Custom Settings

Each domain can be configured for a range of advanced custom configuration settings. There may be a Configuration Fee for these changes – please check with your Bizo account manager or Bizo Support to confirm this when requesting the changes.

Essentially Bizo Email Filter can be configured with a customer setting for your specific domain or individual user requirements. This is generally based on either wildcard or specific “from:” address, or “to:” address, or both.

- Dangerous Content Scanning
- Block Encrypted Messages
- Block Unencrypted messages
- Allow Object Codebase tags
- Allow iFrame Tags

- Allow Form Tags
- Allow Script Tags
- Allow Web Bug Tags
- Archive Mail
- Spam Actions
- High Scoring Spam Actions

3.15 High Availability Features

High availability features are based on SMTP protocol specifics. This technique utilizes "lesser priority" MX DNS records and allows the standby server to process mail traffic immediately after a primary server failure or connectivity loss.

Since there is no vital customer data stored on the server except user settings and account information (mail is not stored there, it gets forwarded immediately), the synchronization traffic and data loss probability is negligible.

Standard architecture of primary servers is fully redundant RAID1.

3.16 Virus Rules

By default emails that are identified as having a virus are not delivered at all. Research has shown that less than 1% of viruses in the wild can be successfully disinfected, so this option is set to "no" by default.

Note that this is not the same as cleaning a message, which removes the infected attachment and delivers the message.

Silent Viruses are also not delivered. (Silent Viruses are viruses that forge the email address of the sender). The system will not send the cleaned virus message to the recipient as these messages are typically useless and are just misleading content generated by the virus itself.

3.17 Virus Signature Updates

The system continually checks for virus alerts and new virus updates. The maximum time between each cycle is less than 10 minutes. Updates from anti-virus vendors are automatically transmitted to all servers.

In the event that a virus alert has been issued, but signatures are not available, the Technical Operations Team has direct access to the rules database and can update instantaneously, hence immediately protecting all users. Note this is in addition to the heuristics anti-virus engine automatically trapping unknown viruses as standard.

3.18 Notification Rules

Bizo Email Filter is configured to send (or not send) the following notification alerts based on current security recommended best practice:

- No - Notification to Senders of Viruses.
- Yes - Notify Senders of Blocked Filenames or Filetypes. This rule sends a notice to the sender of a message that was rejected because it contains Filenames or Filetypes that are blocked by Bizo Email Filter.
- Yes - Notify Senders of Other Blocked Content This rule sends a notice to the sender of a message that was rejected because it contains blocked content.

3.19 All Standard Mail Formats Supported

The mail delivery is standard SMTP, so customers may use almost any mail server. TLS encryption may optionally be used under separate agreement.

MIME and UUENCODE attachments are supported, including all widespread archive formats. Encrypted messages and attachments are not scanned by the system.

3.20 Ongoing System Supervision and Performance Monitoring

The Bizo Email Filter delivery environment is constantly monitored with custom designed software both internally and externally. All unusual data and performance statistics are subject of event-driven immediate human review.

3.21 User Self-Management

Virtually every anti-spam system available uses the concept of Junk Mail Folders. The concept being that the anti-spam system somehow 'tags' the message as spam, so that the users email client removes spam from the main Inbox and places it in an alternative folder.

The downside is this: NO anti-spam filter is ever perfect. There WILL be false positives, and good emails will get inadvertently placed in with all the junk. This means, the user must

remember to search through the junk mail folder, daily, to check for missed good emails. Furthermore, the junk email – often offensive and unpleasant content – has STILL been delivered to the users' PC.

Bizo Email Filter is different. It does not use junk mail folders. Bizo Email Filter stops spam being delivered to user. Instead of requiring the user to search a junk mail folder, Bizo Email Filter delivers a daily email, to each user, which lists the messages caught as spam.

In addition to the daily Quarantine Report email, users can log in to the Bizo Email Filter website to manage their quarantine in further detail. The website offers a wider range of spam management options including:

- Release from Quarantine
- Release to an alternative recipient
- Delete from Quarantine
- Teach the Bizo Email Filter database that a message should be recognized as spam.
- Teach the Bizo Email Filter database that a message should not be recognized as spam.
- Teach the Bizo Email Filter database that a message should be recognized as spam and report to global spam management services (spamhaus.org).
- Teach the Bizo Email Filter database that a message should NOT be recognized as spam and report to global spam management services (spamhaus.org).
- Examination of quarantined email headers in detail.
- Management of individual spam settings
- Management of individual white lists.
- Management of individual black lists.

The Bizo Email Filter self-management system is a powerful way for individual users to gain control over their inbound email, while at the same time receiving the benefits of the sophisticated and efficient anti-spam technology.

Bizo Email Filter removes the need for the customer IT staff to administer the system – users can 'self-serve': no more calls to the internal helpdesk!

3.22 Anti-Porn Filter

Bizo Email Filter uses a unique method to remove pornographic image spam, based on analysis of embedded URL calls in an email.

3.23 Customer Administrator and User Guides

Once your email domain is configured Bizo Support will email your nominated email domain administrator with your access details to log in to the Bizo Email Filter website.

Once you have logged in you will see the link to download or open your user guide (as a PDF file). Your domain administrator also has access to the domain administrator guide.

3.24 Content Policy Management

The Content Policy Management features of Bizo Email Filter fall into two main areas – Content Filtering and Attachment Management.

Attachment Management

Attachment management involves analysis of the MIME parts of each email, with specific reference to the internal data structure. There are two categories of attachments to be controlled – ‘Suspicious’ and ‘Dangerous’. The customer has ability to configure for himself which types of extension fall into which group. However, to make set-up easy, the system has default selections available for High Security, Medium Security and Low Security.

- If an email arrives with an attachment in the Dangerous category, the email is blocked and quarantined.
- If an email arrives with an attachment in the Suspicious category, the email is blocked and quarantined IF THE ATTACHMENT TYPE AS ANALYSED DOES NOT MATCH THE DECLARED TYPE.

The Suspicious category is very useful for identifying and trapping new worm outbreaks and other malicious code which spreads by being ‘hidden’ in executable files MASQUERADING as a different file type.

3.25 Content Filtering

Content filtering is applied to the message body and subject fields, when the message has text or HTML content. The customer may define certain words or phrases, which if found within the email will cause that email to be blocked and quarantined.

The facility for Content Filtering is activated, per user, by the customer administrator. Rules are at either the individual level, or the domain level, and the customer administrator can select which will have priority.

Content Filtering rules can be applied in combination with Attachment Management rules – for example, block and quarantine if the attachment is a password protected archive and the word 'password' appears in the body text.

Content Policy Management rules can be set for both Incoming and Outgoing messages. This allows the customer administrator not just to manage inbound threats, but enforce an internal policy about subject matter and materials being sent outside of the organisation.

3.26 Bizo Email Filter Summary

The following table summarises the service functions provided by Bizo Email Filter:

Bizo Email Filter Feature Summary	
Anti-Spam Engine	
Core Technology	Proprietary
Effectiveness quoted best case	99%
Accuracy (False Positives) quoted best case	0.0001%
Pornography Filter	YES
Email Delivery Assurance	
Whitelist & Blacklist	YES
Spam Quarantine	YES
Per-User Controls	YES
User Notifications	YES
Per-User Email Forward / Relay / Reject	YES
Challenge Response Messaging	YES
Anti-Virus Engine	
Number of A/V Engines	2 +
Heuristic A/V Technology	YES
Dynamic Outbreak Management	YES

System Features	
Class-of-Service Management	YES
Multiple Domains Management	YES
Directory Harvest Attack Protection	YES
Content Policy Management	
Content Filtering Rules	YES
Attachment Blocking Rules	YES
Separate Rules Inbound / Outbound	YES
Optional Domain or Per-User Precedence	YES

3.27 Integration with other Bizo services

Bizo Email Filter is one of a number of Bizo services. While you can subscribe to Bizo Email Filter by itself, for ease of use Bizo Email Filter integrates tightly with the other Bizo services.

Bizo also offers a variety of pre-packaged managed services from single subscription-based hosted services such as Business Messaging, to comprehensive and ready-to-deploy solutions for a wide range of business needs. Adding or deleting any additional services is an easy and template-driven process.

The available Bizo service suites are described as follows. “Get Connected” is the Bizo network connectivity suite; “Get Secure” is the Bizo security suite, and the final section summarises the Bizo “Get Working” suite of business services.

A service description for each service is available for download from the Bizo website (www.bizoservices.com).

3.27.1 Get Connected

- Bizo Internet

3.27.2 Get Secure

- Bizo Defend Perimeter
- Bizo Defend Integrity Desktop

- Bizo Email Filter
- Bizo Web Filter
- Bizo Backup
- Bizo Systems Monitor

3.27.3 Get Working

- Bizo Business Messaging (Bizomail Lite and Bizomail Standard)
- Bizo Payroll
- Bizo BackOffice
- Bizo SharedDrive

3.27.4 Get Talking

- Bizo Local Access
- Bizo Tolls
- Bizo Central PABX
- Bizo Virtual Reception
- Bizo Telemarket

3.28 Quality Assurance and Change Management

Bizo operates a strict QA system to ensure compliance with the future objective of ISO quality accreditation. All policies and procedures are fully documented, recorded and controlled.

Quality is taken as individual responsibility throughout the organisation, from CEO downwards. Service changes are managed through strict adherence to the Bizo ITIL-based Change Management process.



3.29 Ongoing System Supervision and Performance Monitoring

The Bizo Email Filter delivery environment is constantly monitored with custom designed software both internally and externally. All unusual data and performance statistics are subject of event-driven immediate human review.

4. Is Bizo Email Filter for you?

Bizo Email Filter is ideal for businesses that have invested in an in-house email system (such as Microsoft Exchange™, for example) but cannot justify the additional expense to implement and maintain email security, spam and pornography management technology.

Bizo Email Filter provides a business-grade enhancement for low-end ISP-email consumer-type services giving a commercial assurance against malicious attacks and unwanted emails.

Bizo Email Filter is a great fit for your business if:

- You have an in-house email system but need better email virus, spam and pornography protection.
- You have an in-house email system and would at some stage like to move entirely to Bizo Business Messaging but need some interim protection that does not require additional capital, technical experience or time.
- You have an in-house email scanning system but the cost of support, maintenance, upgrades and a corporate-style fully resilient data-centre housed design cannot be justified.
- Your business subscribes to a low-cost consumer ISP-based email service but you need a commercial assurance and protection against unwanted and malicious email attacks.
- You want better management of staff email security and content but can't justify the in-house expense or effort.

5. What are Your Responsibilities?

To make the most of Bizo Email Filter it is important that you familiarise yourself with the specific service requirements and the Bizo support and service policy and processes. The key customer responsibilities are described below.

5.1 Bizo Service Offer and Terms

This document is the contract between Bizo and our customers for the provisioning and supply of Bizo services. Please read this carefully and discuss any questions with Bizo sales staff.

5.2 Unique Mail Domain

All we need to technically implement Bizo Email Filter for you is your email domain name, your nominated email domain administrator, and the redirection of your email domain MX record. We can either make the changes to your MX record on your behalf, or you can arrange for the MX record to be redirected by your domain administrator.

5.3 Acceptable Use Policy

The Internet is a very large community of computer users. As with any community it is important that we work together and avoid harm to each other. Bizo has a standard Acceptable Use Policy which is published on our website (www.bizoservices.com). This policy details the ways in which the Bizo services must and must not be used. This policy helps safeguard Bizo customers and other Internet and network users.

5.4 Privacy Policy

Bizo takes responsibility for looking after your information very seriously. The Bizo Privacy Policy is also published on our website (www.bizoservices.com) and describes our commitment to the privacy and security of your information.

5.5 Support

Please report any service faults as soon as you can. In every likelihood our 24 x 7 monitoring service has already identified the fault and staff are working to remedy. You can contact the Bizo Support Desk by emailing or by phone, please see the website for access details.

Remember that if you don't let us know it is harder for us to help you.

You can subscribe to new Bizo services or additional features to existing services via the Bizo Self Service Portal online interface.

9. Copyright Information

Both downloadable and on-screen documentation are free to view in electronic form via your World Wide Web browser, however Bizo maintains their copyrights. You are entitled to make one copy for research purposes, however you may not further copy or republish them or store them in your computer or elsewhere except as required by your browser for the sole purpose of viewing them while using the browser.