

PART D - BRIARS SECURE MAIL SERVICE

1. CONTRACT TERMS

- 1.1. These are the additional terms on which we will provide the Briars Secure Email Service to you (the "Service"). These terms and conditions form an integral part of the agreement between us and accompany the General Terms set out in Part A above ("the General Terms"). In the event of conflict between the General Terms and this Part D, the terms of the Part D shall prevail. "Terms and Conditions" means the General Terms (Part A) as amended by these Special Conditions (Part D).

2. ACCEPTANCE

- 2.1. Acceptance by you of delivery of the Products shall (without prejudice to condition 2 of the General Terms or any other manner in which acceptance of these Conditions may be evidenced) be deemed to constitute unqualified acceptance of these Conditions.
- 2.2. A variation of these Conditions is valid only if it is in writing and signed by a director or our authorised representative.

3. DEFINITIONS

- 3.1. The following words or expressions have the following meanings:-
 - 3.1.1. the "Minimum Period" means, in relation to the Service, the period of twelve months beginning on the date after the service has been made available to you and ending on the first anniversary of such date;
 - 3.1.2. the "Service" means the Secure Email Service as operated by Briars from time to time and more particularly described in the clauses 11 and 12 of these Special Conditions;
 - 3.1.3. the "Software" means the anti-virus software licensed to and used by us in connection with the Service from time to time; and
 - 3.1.4. "virus" means a piece of code usually (but not necessarily) disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is designed so that it may automatically spread to other computer users.
 - 3.1.5. "Email" means any electronic message generated by an End-User and sent or received via the Service generally in a business-to-business environment over the World Wide Web generally understood as the "Internet".
 - 3.1.6. "End-User" means a specific E-mail account or mailbox managed by or on behalf of a Customer and configured to send or receive E-mail via the Service.

4. SERVICE

- 4.1. In consideration of you paying our charges from time to time, we agree to supply the Service to you. Please refer to Clause 7 below and our exclusion/limitation of liability in this regard.
- 4.2. We will use our reasonable endeavours to maintain and update the Software as soon as our licensors make any appropriate upgrades or enhancements to the Software.
- 4.3. We recognise and confirm that the content of all E-mails

scanned on your behalf by the Service is confidential. In the normal provision of the service we would not access, read or copy E-mails or their attachments other than by electronic methods for the purposes of virus scanning. However, we reserve the right to utilise the virus related content of the E-mail or its attachments solely for the purposes of:

- 4.3.1. maintaining and improving the performance and the integrity of the Service;
- 4.3.2. observing, studying and/or testing the functioning of the Service;
- 4.3.3. complying with all regulatory, legislative or contractual requirements; and
- 4.3.4. making available to our licensors of the Software any information passing through our systems which may be of interest to our licensors solely for the purpose of further developing and enhancing the Service.

Where we exercise our right in this matter we will use all reasonable endeavours to keep confidential information received by us from you or for you in connection with the Service.

- 4.4. Virus-infected E-mails, which are stored in our holding area will be deleted after a period of 30 days. Should you require us to transmit a virus infected E-mail to you from the holding area, this will be done at your risk and we will take no responsibility whatsoever for any loss, corruption or failure of any data or systems. We will under no circumstances transmit any such virus infected E-mails to third parties on your behalf.
- 4.5. We reserve the right both prior to the provisioning of the Service and at any time during the supply of the Service to test whether your E-mail systems allow Open Relay. If at any time your E-mail systems are found to allow Open Relay, we will inform you and reserve the right to withhold provision of or suspend all or part of the Service immediately and until the problem has been resolved.
- 4.6. Subject to applicable legislation, Briars may provide the Service from any of its hardware installations anywhere in the world and may, at any time, transfer the provision of the Service from one installation to another. Briars does not guarantee that any such installation, or part thereof, is dedicated to your sole use.

5. CUSTOMER'S OBLIGATIONS

- 5.1. In consideration of us supplying, or procuring the supply of, the Service to you, you agree to pay our charges from time to time in accordance with Clause 6 of this Part and Clause 6 of the General Terms.
- 5.2. You will supply us with all technical data and all other information we may reasonably request from time to time to allow us to supply the Service to you. All information you supply will be complete, accurate and given in good faith. You hereby authorise us to make all necessary changes to your DNS records for the purpose of making the Service available to you.
- 5.3. If you are not transferring your Domain Name/s to Briars, you will be contacted by us shortly after your Registration Agreement has been received and we will explain to you the necessary changes you (or your ISP) will need to make to your mail server so that your mail can be scanned. We shall not be liable to you for any delays caused by you (or your ISP) not carrying out our instructions and we reserve the right to commence charging for the Service in accordance with the General Terms.

PART D - BRIARS SECURE MAIL SERVICE

6. CHARGES AND PAYMENT

- 6.1. The charges for the Service are applicable to normal use of the Service by End-Users. We define "normal use" for an End-User as sending and receiving e-mail messages and attachments in the execution of the Customer's business. We reserve the right to apply charges to you for any use of the Service that adversely affects the general performance of the Service whether intentional or not, such charges to reflect the cost of rectifying any fault caused by the Customer's use of the service
- 6.2. The invoiced amount shall relate to the number of End-User Email accounts operated by the Customer on the commencement of the service.
- 6.3. We will monitor your usage of the Service on a monthly basis and reserve the right to make adjustments to our charges in line with actual usage of the Service.

7. TERMINATION

- 7.1. Both parties' rights of termination and cancellation shall be as set out in the General Terms.

8. DATA PRIVACY AND REGULATION OF INVESTIGATORY POWERS

- 8.1. You shall take all necessary measures to ensure that you, and all of your End-Users, are aware of any responsibilities they have in respect of data protection and privacy laws and/or regulations and as we have no control or influence over the content of the E-mails processed by the Service you shall hold us harmless for any claims by any party relating thereto.
- 8.2. As required by law, you shall use all reasonable efforts to ensure you inform (for example via a banner message on E-mails) End-Users and others who use any communications system covered by the Service, that communications transmitted through such system may be intercepted, and indicate the purposes of such interception. You shall hold us harmless from any claims from End-Users, any third party and/or governmental agencies relating to such interceptions. You shall not use, or require us to use, any data obtained via the Services for any unlawful purposes.

9. WARRANTY AND LIABILITY

- 9.1. Provisions relating to warranties and liability are set out in Clauses 8 and 9 of the General Terms.

10. SERVICE LEVELS AND REFUNDS

- 10.1. If in any calendar month the availability of the Service (other than for reasons of Force Majeure or third party faults) is calculated by us to fall below 99.5% you may be entitled to a credit against the monthly charges invoiced to you for that calendar month.
- 10.2. If our whole network or a part thereof fails preventing all Services to you from being operational we will measure Non-availability from the time the network or part thereof experiences a failure to such time as services are restored to you. Periods of Non-availability will be measured by our internal system logs and excludes periods of scheduled maintenance as specified by us from time to time.
- 10.3. In the event that you believe you are entitled to compensation and in order to obtain your credit simply

notify us that you think you are so entitled and we will check our Non-availability records, compare it against any critical calls we previously received from you at our Helpdesk and confirm whether any credit is due. In the event we decide credit is due, your entitlement will be determined as follows: For any period of non-availability in a calendar month, you will be entitled to a credit equivalent to the monthly charges due from you in that month, subject to a maximum of 100% of the monthly charges in any calendar month.

- 10.4. The remedy set out in this Clause 10 shall be your sole and exclusive remedy in contract, tort or otherwise in respect of non-availability of Service.
- 10.5. Notwithstanding the provisions of this Clause 10, in the event that average Service availability falls below 89.5% in any calendar month, you shall be entitled to terminate this contract forthwith. Such termination shall be your sole and exclusive remedy in contract, tort or otherwise with respect to such Non-availability of Service.
- 10.6. You agree that we are not liable in respect of any non-availability that results from any event of Force Majeure, and acts or omissions by you or your staff/officers/agents/contractors that is in contravention of the Terms and Conditions or from the acts or omissions of any third parties.

11. THE SERVICE

11.1. The Service

Briars Secure Email Service

11.2. Service Description

The Service will scan as much of the Email and its attachments as possible and where a Virus is detected will follow the procedure set out in Clause 3 below. It may not be possible to scan attachments with content which are under the direct control of the sender (for example, password protected, encrypted and/or some types of compressed attachments).

11.3. Procedure

- 11.3.1. If a Customer's inbound or outbound Email or attachments are found to contain a Virus, an automatic alert will be despatched to the sender by way of notification. Notification will also be sent to a Briars system administrator in both cases. The infected Email is quarantined in a holding area pending destruction after thirty (30) days.
- 11.3.2. Briars continuously monitor Email queue lengths. If a rising Email queue is detected for a connected domain, Briars will test for the ability of the receiving mail server to receive Email. If this test fails, the affected party will be notified. If Briars is unable to deliver Email to a customer's mail server Briars will store the Customer's inbound Email for up to seventy two (72) hours pending delivery.
- 11.3.3. The average scanning time through the selected anti-Virus filters is less than 2 seconds, based on processing a 1MB Email (including attachments) under normal operating circumstances.
- 11.3.4. The flow of Email traffic in any given period may have great variance for reasons that are beyond the control of Briars. For this reason, Briars cannot guarantee service levels. As a guide to the level of service to be expected: typically the maximum processing time including inbound queuing routine and scanning to first delivery attempt is 30 seconds for 99% of Emails processed, with the remainder being processed within 15 minutes.

11.3.5. The Service is designed with inbuilt high capacity, resilience and scalability. Hardware is sourced from industry-leading suppliers known for their approach to quality and their high Mean Time Between Failure (MTBF) ratings. Individual mail servers are configured to maximise redundancy for mission critical items. Server hosting is carefully chosen using server centres where continuity of service and security are paramount. Briars have back-to-back service level agreements with all the providers of server hosting. The network configuration is designed to provide resilience in the unlikely event of the loss of any individual segment of the network.

11.3.6. Wherever possible, planned maintenance by Briars will be carried out without affecting the Service. This will generally be achieved by carrying out planned maintenance during periods of anticipated low Email traffic and by carrying out planned maintenance on part, not all, of the network at any one time. During planned maintenance periods the Email traffic will be diverted round sections of the network not undergoing maintenance in order to minimise disruption to the Service.

11.4. Email Reporting

Briars will provide the Customer with a designated Email address for the reporting of all support issues relating to the Service. From time to time and at its discretion Briars may send reports to the Customer relating to the performance and operation of the Service.

11.5. Releasing a Virus Infected Email

Briars will only release Virus infected Email upon receipt of the appropriate Release Authorisation Form from the Customer. Briars will only act on a request authorised by the Customer to forward Virus infected Email to the address specified on the Release Authorisation Form. Briars will not return Virus infected Email to the sender. Briars will not forward Virus infected Email to third parties.

11.6. Maximum Mail Sizes Handled By The Service

There is currently a maximum message size of 25 MB on any Email including attachments.

12. SUPPORT SERVICES

12.1. Hours of Operation

Support services are available through our Technical Helpdesk which is operational Monday to Friday from 9am to 5pm. Out of hours support (i.e. 24hrs x 7 days per week) may be arranged in respect of critical incidents only. If we subsequently find that an out of hours call is not critical, you will be charged for the services provided at our prevailing rates then in force. On-site technical support can be provided by arrangement at prevailing rates.

12.2. Technical Support Procedures

12.2.1. Upon reporting the incident (via the telephone or email), the incident will be assigned a unique support ID number which should be quoted in future correspondence.

12.2.2. In the event our Support service is not able to help you immediately, your request for service will be logged and we will endeavour to respond to you as defined by the severities below.

Severity	Description	Service Level Response
1 – Critical	Total Service is unavailable	1 Working Hour
2 – Major	Partial Service, an element of the total service has failed	2 Working Hours
3 – Minor	Impaired service, no element has totally failed but there is a quality issue with one or more element	4 Working Hours
4 – Request	The service is unaffected. Customer request for product related technical advice	1 Business Day

12.2.3. This table reflects the initial response times within which an engineer will endeavour to respond to you. Incident resolution may require multiple communications and off-line research before being brought to fruition.

12.2.4. If, upon investigating the cause of the incident, we determine there is a defect in the Products, we will try to provide a remedy in the form of a workaround, or another version of the Products that includes a bug fix for the specific defined problem.

12.2.5. Our success in resolving incidents is conditional upon your willingness to follow our instructions with regards to installation, operation and the use of the Products. You shall agree to implement corrective actions and workaround procedures recommended by us to resolve the incident. We will not be liable for any defaults in the Products that result from your failure to execute a supplied corrective action.

12.2.6. You are responsible for providing support information necessary to understand and resolve the incident. This information may include the following: log files, configuration files and error messages. Timely receipt of such requested information is key to expediting the troubleshooting process.