IGNITE SECUREMAIL

PLEASE NOTE: These product or service specific terms and conditions must always be read together with our General Terms and Conditions, which will always apply to your use of this product or service.

TERMS AND CONDITIONS OF SERVICE

1. Definitions

1.1. **"Agreement"** means this document together with the Ignite General Terms and Conditions.

1.2. "**Active User"** means any email address on the clients domain which receives 22 (twenty two) or sends 1 (one) Clean Email within the previous month;

1.3. **"Clean Email"** is an email that is not deemed as spam or harmful by the service.

1.4. **"Client"** means the person(s) registered on www.ignite.co.za;

1.5. **"Fees**" means the amounts payable by the Client in accordance with the relevant units or quantities relevant to such Services (such as number of Users, gigabytes etc) as specified on www.ignite.co.za ;

1.5.1. "**Upfront Fees"** means fees payable by the Client prior to the commencement of the Services and as otherwise agreed to by the Parties;

1.5.2. "**Monthly Fees"** means fees payable by the Client monthly in advance.

1.5.3. **"Quarterly Fees"** means fees payable by the Client quarterly in advance unless otherwise agreed to by the Parties in writing;

1.5.4. **"Annual Fees"** means fees payable by the Client annually in advance unless otherwise agreed to by the Parties in writing;

1.6. **"Overage Fees"** means monthly fees payable in arrears by the Client for additional units or quantities, related to their Service(s), that are in excess of the initial amount(s) stipulated in their Proposal.

1.7. **"Proposal"** means the Proposal submitted to the Client by the Service Provider and the Proposal Summary which records the material terms of the Services as agreed to by the Parties and signed by the Parties;

1.8. **"Service"** means current and future active Service(s) rendered by Ignite to the Client as set out in the Proposal;

1.9. **"Users"** means the Client's personnel or other specified persons permitted to access or use the Services and restricted in number but subject to change from time to time, the accurate number of permitted persons may be requested from Ignite from time to time.

2. Services

2.1. ***Services Packages:*** The Ignite Securemail Service comprises, as applicable to the Client and specified in the Proposal the following package

Service Description
Securemail advanced email security for inbound and outbound email

2.2. ***Service Features:*** The IGNITE Securemail Service comprises, as applicable to the Client and specified in the Proposal the following features:

Features	Detail
Email filtering	• Filtering of inbound and/or outbound email for spam, viruses and phishing attempts. • Blocking of (i) configured file types and (ii) emails based on size of email restrictions.
Email spooling	• Spooling of email for up to 14 days if the destination mail server is unavailable.
Smart host for outbound mail	• Mail relay services offered on the IGNITE Securemail outbound service • Mail relaying secured via a choice of (i) SMTP authentication or (ii) source IP address
Reporting	The Ignite Securemail interface provides detailed reporting on: • Audit trails of system events: includes user logins, reports generated, emails viewed and/or released from the quarantine • Email analysis reports by domain, sending or recipient: includes percentage of email classified as clean email, spam, viruses; total data processed; total data delivered • Sender / recipient analysis reports: includes breakdown of top senders or recipients by mail count and mail volumes
Blacklists and Whitelists	• Blacklists and Whitelists configuration to and/or from an email address and/or domain
Email Quarantine	• Quarantine of emails classified as spam for 30 days. • Ability to release emails from the quarantine.

Spam training system	• Ability to train the system to relearn email as clean or non-clean
Domain wide service	• Ignite Securemail is a domain-based service. This means that an entire email domain (e.g. synaq.com) is configured for this service. • The service cannot be configured for a subset of Users on a domain.

2.3. ***Exclusions:*** The following features, products, support and services without limitation are excluded from the Ignite Securemail Service:

2.3.1. Internet connectivity and support services related to Internet connectivity (please contact your Internet service provider);

2.3.2. Hardware required to access the Service (such as computers);

2.3.3. Destination email server and the support related to such server;

2.3.4. The ability to reroute of email to another destination when the original email server becomes unavailable;

2.3.5. Ability to read email spooled on the system;

2.3.6. Ability to integrate with an external directory service such as LDAP or AD;

2.3.7. End user training and support not specifically provided for in the Proposal; and

2.3.8. Any support, services, features or products not explicitly stated in the Proposal.

3. Limitations and Technical Requirements

3.1. SMTP AUTHENTICATION REQUIREMENTS

3.1.1. Securemail offers its clients two methods of SMTP Authentication for outgoing email transmission, namely:

3.1.1.1. SMTP Authentication with a Username and Password. This method is normally implemented using a Smart Host configuration implemented on the client's on-premise email services, but in certain circumstances it may be implemented on a per-sending user basis.

3.1.1.2. IP Address Authentication, where a client's provisioned email domain or domains are allowed to relay mail outbound from a client's static public IP Address or range of IP Addresses, without the need to use SMTP Authentication (as in 1 above). MINIMUM REQUIREMENTS FOR SMTP AUTHENTICATION WITH USERNAME AND PASSWORD PER SENDER ADDRESS

3.1.2. Securemail requires that clients create SMTP Authentication passwords using at a minimum, the following password policy:

3.1.2.1. Minimum password length = 8

3.1.2.2. Minimum upper case characters = 1
3.1.2.3. Minimum lower case characters = 1
3.1.2.4. Minimum punctuation symbols = 1
3.1.2.5. Minimum numeric characters = 1

3.2. SENDER VERIFICATION ON THE CLIENT'S SERVER

3.2.1. When using either of these methods the client's mailbox server must support Sender Verification in the form of a SMTP Protocol lookup, to confirm a sender is indeed a valid and real mailbox or email alias on their mailbox server.

3.3. SMTP TRANSMISSION LIMITS

3.3.1. Securemail is not a bulk email service. However, Ignite will allow its clients, on a case-by-case basis, to declare named bulk-sending email addresses. In such cases, Ignite will then engage in negotiations with the client to provide specialised bulk mail routing for these accounts to ensure the client's business needs are met while the Securemail system as whole and its other clients are not adversely affected.

3.4. SMTP - MESSAGE RECIPIENT LIMITS

3.4.1. No more than 50 recipients per message.
3.4.2. No more than 200 recipients per sender address per 5 minutes.

3.5. SMTP – MAIL SUBMISSION RATE LIMITS:

3.5.1. Mail throttling, (implemented as a SMTP temporary defer) is enforced by Securemail when the following submission rates are exceeded:

3.5.1.1. Submission exceeds 200 emails per sending host per 5 minutes.
3.5.1.2. Submission exceeds 200 emails per sender address per minute.

3.6. USE OF EMAIL ADDRESS LISTS

3.6.1. Ignite will not discourage the use of sending to email address lists, provided that all lists only consist of valid and legitimate contacts and do not contravene the Unsolicited Bulk Email (UBE) or Unsolicited Commercial Email (UCE) regulations as stipulated in the AUP.

3.6.2. Any sending address or SMTP username which routinely, or excessively exceeds the threshold for invalid recipient addresses will be considered as sending UBE or UCE, and the account will be locked out to protect other users and to protect the integrity of the Securemail service.

3.7. SMTP - INVALID RECIPIENT LIMITS

3.7.1. No more than 2 invalid recipients per message.
3.7.2. No more than 10 invalid recipe ents per sender address per 5 minutes.

3.8. DOMAIN RELAY LIMITS

3.8.1. Securemail will only relay email for domains that are owned by and registered to the client.

3.8.2. Securemail will not relay any Freemail or Internet Service Provider generic domains E.g. gmail.com, yahoo.com, hotmail.com, telkomsa.net, webmail.co.za etc.

4. ***Delivery of Service:***

4.1. Securemail Inbound, clean email is delivered via SMTP to the customer's mail server.

4.2. Securemail Outbound, email is delivered via SMTP from the customer's mail server.

4.3. Securemail reporting interface is offered via the World Wide Web via www.ignite.co.za

5. Charges and Payment

5.1. Securemail will be billed monthly in advanced based on the number of Active Users.

6. Termination

6.1. The duration of the service shall endure for a 1 (one) month rolling period until terminated by either party on 30 (thirty) days' notice.

7. ***Indemnifications, Limitation of Liabilities, Warranties:***

7.1. The Client hereby indemnifies and holds Ignite harmless against any loss, claims, demands, proceedings, damages and expenses of whatsoever nature arising from:

7.1.1. Errors by the Client when requesting or effecting changes to the Domain Name System and any resulting delay, rejection or loss of email;

7.1.2. Misconfigurations by the Client of destination email servers and/or firewalls irrespective of whether Ignite has instructed the Client or Users on how to configure such servers or firewalls unless Ignite is the Client's appointed Email Service Provider, and has attended to the above configurations;

7.1.3. Ignite's third party dependencies for the provision of the Service including without limitation: Internet connectivity, power, air conditioning at the hosting facility; Viruses and Spam received by the Client notwithstanding use of Ignite Securemail;

7.1.4. Actual delivery of outbound email to final destination due to circumstances beyond Ignite's control including without limitation: unavailability of the destination server, the email recipient address is incorrect/ does not exist, the User has exceeded the limits placed on use of the Service, spam filtering)

7.2. The maximum liability of Ignite to the Client in terms for any one event or series of connected events above, shall in accordance with the provisions of the General Terms and Conditions.