# The Email Laundry

## Email Security Service

## *Service & Data Security Policies*

The Email Laundry is committed to ensuring the security of our customer's data.

As such, we implement, enforce and audit procedures to adhere to customer service and data security policies.

## Physical Security

- Geographically-dispersed data centres
- Restricted access
- Security surveillance
- Climate controls & fire detection systems
- Uninterrupted power supplies

The email security service is provided across multiple geographically-dispersed data centres within the EU. This ensures that there is no single point of failure should any systems within a data centre or a complete data centre itself become unavailable.

Physical access to the data centres is highly-restricted and permitted only to authorised employees. Entrances and server rooms are monitored by closed-circuit TV cameras.

The data centres provide climate control to regulate the operating environments, with fire and smoke detection and fire suppression systems in place. Additionally, uninterrupted power supplies with backup generators ensure power supply.

## Technical / Network Security

- Multiple redundant connections to internet exchange points
- Best-of-breed hardware at network and server level
- Firewalled access and intrusion detection monitoring
- Vulnerability / threat testing and patch management
- Encryption of data in transit and at rest

Service data centres use multiple redundant connections to internet exchange points to ensure no loss of connectivity and service in the event of upstream links going down.

All servers are firewalled to restrict access at a network level while intrusion detection systems are in place to monitor unauthorised access. Vulnerability testing is carried out at regular intervals to ensure any vulnerability is identified and patched as quickly as possible.

TLS encryption for inbound and outbound SMTP relay is employed for customers where required. Specific customer data is encrypted when stored on our network infrastructure.

## Administrative Security

- Service controls
- Service auditing

Employees have no access to customer email being relayed through the services.

To provide support to customers, access to limited logging information about email delivery is made available to support staff.

Changes to service configuration settings are fully logged for auditing purposes.

## Data Protection

- Service controls
- Service auditing

Any personal information saved on our network infrastructure is used exclusively in the provision of services and for billing purposes.

Employee access to customer personal information is restricted, with employees contractually obliged not to disclose internal business information to third parties.

Employee training in data protection policies is carried out on a continual basis.



Clean Communications Ltd

uk. +44 (0) 208 099 3796 | us. +1 617 963 8322 | tel. +353 (0) 45 897766 | e.info@TheEmailLaundry.com | w.www.TheEmailLaundry.com