



## **Fire Suppression**

Data centres are built with robust fire protection systems.

## **Environmental Controls**

Data centres provide power and cooling systems that are provisioned with appropriate redundant failover infrastructure. The power and cooling infrastructure is backed up by an emergency power generation system.

## **TECHNICAL CONTROLS**

### **Network and System Security**

Multiple levels of disparate defences are used to help protect customer information and control network access. Only inbound connections from Web browsers via 128-bit SSL and on-premise software components are allowed. All access to servers is monitored. In addition, servers are configured to provide protection against intrusions and day-to-day threats. The servers are selected and configured to improve their reliability, security, scalability and efficiency.

### **Data Transmission**

Customer Data is transmitted to data centres using Secure Sockets Layer (SSL) with 128-bit encryption designed to protect against unauthorized access from third parties, loss and fraud. This protocol enables authentication, data encryption and message integrity. All connection to Email Archiving and Email Continuity services is outbound from the customer to the data centres and is made using an HTTPS connection. Archive mail transfer occurs via outbound SFTP connection using AES-128.

### **Authentication**

Automated data transfer mechanisms authenticate with Hosted Email Archiving and Hosted Email Continuity services using a unique username and password as well as industry standard Certificate Authorities.

User access to Hosted Email Archiving and Hosted Email Continuity services occurs via a secure Web interface and Secure Socket Layer (SSL) connection encrypted with the same 128-bit SSL protocol. Users are required to enter a username and password before accessing the system. If an incorrect username or password is entered, then access is not granted. Customers can define password strength and reuse rules, as well as account lockout policies.

Remote administration is performed over an encrypted VPN session that requires a username and password. Any attempts to access the system with an incorrect password are rejected and logged.

To access email and Customer Data, users must provide a username and password. The Hosted Email Archiving and Hosted Email Continuity services will allow access only to the specific information that is authorized by the provided credential. In addition to access controls, a pass phrase is also required when a request is made for MessageLabs to activate the Hosted Email Continuity system. This prevents unauthorized activation of the Hosted Email Continuity system.

### **Authorization**

Although data center personnel will have physical access to the Hosted Email Archiving and Hosted Email Continuity services equipment for emergency purposes, they have no access to the data contained within those systems.

Authorized access is granted to the customer and MessageLabs support. Through multiple layers of access control, customers are only allowed to access their own information. The system is designed to prevent one customer from viewing data from another customer. Controls are put in place at the operating system level and the application level to prevent unauthorized access. Although administrators can view some Customer Data, there are policies in place that dictate this can occur only for troubleshooting purposes. Prior authorization is required from the customer before any access

