StrikerCLOUD understands that business email and related information is highly sensitive. This is why we have implemented strict procedures and processes in order to safeguard valuable data in regards to our hosted email and collaboration offering, systems, and related operations. Our list of security controls pertains to Organizational Structure, Physical Security, Data Backup, System Availability, Logical Security, Change Management, and Communications.

Here is an overview of these safeguards:

1. **Intrusion systems**

StrikerCLOUD safeguards valuable client data through strict procedures, rigorous processes, and leading-edge security systems. Multiple layers of protection include industry-leading firewalls, intrusion-prevention systems, and advanced anti-spam and anti-virus applications. At StrikerCLOUD, client information is proactively treated at all times with the highest level of security.

In order to secure confidential data, the proposed solution will offer a protection shield comprised of four independent layers. These layers include sophisticated Intrusion Prevention Systems (IPS), world-renowned enterprise-class firewalls, Traffic Control anti-spam applications, and integrated anti-spam/anti-virus appliances. Each component of this shield is redundant and working in load balancing/clustering to offer optimal protection and reliability.

As a first layer of protection, StrikerCLOUD uses the most advanced third-generation family of Intrusion Prevention System (IPS). Designed to deliver non-disruptive protection against constantly evolving threats, it combines stateful firewall, content-based IPS/IDS, and attack mitigation algorithms. The IPS used is one of the only solutions that provide Three Dimensional Protection (3DP) against undesired access, malicious content and rate-based attacks. It provides maximum protection for critical IT assets while allowing full access to legitimate users and applications.

Our security measures are tested at least once a year for intrusion tests.

2. **Firewalls**

In addition to the IPS, StrikerCLOUD uses market-leading firewall appliances for additional protection. Packet filtering, anti-spoofing, and access control lists are enforced at this layer. This additional layer of protection will offer even more security and reliability to users and customers.

The Traffic Controller layer uses sophisticated analytics working at the network's edge to separate legitimate senders from suspicious senders, prioritizing bandwidth and mail server resources for legitimate senders while punishing spammers. The Traffic Control application slows down suspicious email senders, letting legitimate email through while causing impatient spammers to give up. Because spammers require rapid, high-volume delivery to make money, they disconnect after being slowed, looking elsewhere for unprotected targets. This is a completely different and more effective way to stop spam than other so-called traffic-shaping systems, which merely ask suspicious senders to retry later.

Connection between the Outlook workstations and the Microsoft Exchange platform is done via Outlook Anywhere (RPCoHTTPS) which is fully encrypted over SSL. Authentication is done over SSL with Outlook connecting to the Active Directory. NTLM authentication is used.

Management of all security procedures, including personnel permission and access is assured by our strict controls and procedures.

3. Data Center Security

No StrikerCLOUD business partner or contractor has any kind of logical or physical access to any of StrikerCLOUD's production systems. Furthermore, security is enforced through the use of strict entrance control procedures. The data centres key security features include:

- Comprehensive video surveillance;
- Card access to the building, elevators, and data centre;
- Card access restricted areas accessible only by appropriate personnel;
- Cabinets and racks locked with keys and only distributed to required personnel;
- All visitors or third party consultants escorted by authorized personnel.

4. Anti-Spam/Anti-Virus

All incoming emails will be filtered for viruses and malware. The world leading Cloudmark engine is used for virus and malware scanning. Emails containing viruses or malware are detected and eliminated prior to even reaching the Microsoft Exchange platform.

The combination of the MailChannels Traffic Control pre-filter at the connection level with the Cloudmark intelligent content filtering technology allows us to bring you an efficient, accurate, and easy-to-manage anti-spam that offers the following benefits:

- "Zero-hour" rejection of new threats
- Fine-grained management
- Over 99% filtering accuracy
- Organization-wide blacklist and whitelist
- Unmatched reliability

The fast majority of the settings can be administrated at the Company level and/or at the user-level. Users will be able to control spam filtering options (i.e. control level, black list, white list etc.) through their end-user control panel. Finally, Users quarantined items will be located in the "Junk Mail" folder of Outlook from which they will be able to restore or delete items.

StrikerCLOUD's anti-spam/anti-virus firewall is an integrated hardware and software solution designed to protect users from spam, virus, spoofing, phishing, and spyware attacks. This layer of protection includes in itself 12 protection mechanisms and integrates seamlessly with the Exchange 2010 solution. Users have access to their own quarantine to manage recipients. This quarantine interface contains numerous end-user features that allow for individual or organizational tuning and greatly enhance the accuracy of spam filtering.

5. **File backup (mailbox and SharePoint) and level recovery procedures**

StrikerCLOUD understands company email and related information is highly sensitive, which is why it has also implemented strict procedures and processes to safeguard valuable data.

StrikerCLOUD's efficient, reliable and secure backup solution has been designed in order to provide maximum data security. Specifics of the backup solution such as retention and cycle will be refined through due diligence if needed. StrikerCLOUD's backup solution includes (all files within the backups are encrypted):

- Daily backups made on mailbox server passive node to avoid affecting regular email flow and mailbox resources.
- Incremental daily backups that can be configured in shorter cycles such as every few hours if needed.
- Daily backups stored on local SAN to increase restore speed.
- Full weekly backup of all mailboxes stored on remote site tape library and sent off-site in a vault managed by a world leader in data protection.
- Full monthly backup of all mailboxes stored on remote site tape library and sent off-site in vault managed by a world leader in data protection.
- Possibility to restore individual emails, folders, mailboxes, or entire Exchange databases and systems.

StrikerCLOUD tests its backup and restores emails or folders frequently. With hundreds of thousands of mailboxes, mistakenly deleted data by customers is common. Several emails, folders or mailboxes restore are performed each week. Moreover, StrikerCLOUD has a procedure in place to test backups every month. Each restoration is documented for further reference.

Daily backups will be stored in local SAN whereas weekly and monthly backups will be stored on remote site tape library and sent in a vault managed by a world leader in data protection. This process will ensure that the data is available for recovery whenever and wherever needed. The process of online backup to disk also provides for much faster backup and recovery.

Estimated time to retrieve data from Backups located on a SAN is one hour and estimated time to retrieve data from Backups located in the secure vault is four hours.

6. **Archive Solutions**

StrikerCLOUD's proprietary hosted Archiving, email storage is as simple as ABC. Designed to integrate seamlessly with our hosted exchange solution, StrikerCLOUD's enterprise archiving backs up all sent and received emails on your domain. We bring you the affordable and easy to use tool you need to manage the lifecycle of your corporate emails:

- Unlimited storage space
- Unlimited retention period
- Unique control panel
- Instant set-up

StrikerCLOUD's Hosted Archiving acts both as a backup and a retention solution. Since a domain-wide capture of all incoming and outgoing emails is taken, you can easily retrieve lost emails as well as store messages for archival purposes.

StrikerCLOUD's archiving service allows the indexing and preserving of all sent and received emails. Using a thorough list of all message components, emails are fully indexed by message content and attachments with the option to add tags for customized searches. The archive search tool located in the web user interface conducts quick full-text searches based on tags and message content. Users can easily search, view, and forward email archives to active mailboxes.

If you have any questions regarding StrikerCLOUD’s security and safeguard protocols, please do not hesitate to contact us by phone 800-857-4017 or by email: strikercloud@americanopex.com.