GlobalLounge Security (Indicative Guide)

NB: The provisions in this document are provided without legal liability and are subject to change without notice.

In BRIEF:

Global Lounge is a cloud-based transcription workflow system that incorporates the following security applications:

- Data Center - Your server is hosted in a secure environment meeting ISO 27001 security certification standard and PCI DSS standard.
- Firewalls - pfSense based firewalls provide state-full packet inspection to the public traffic destined for the server.
- Redundant storage - Server is configured with RAID 1.
- Backup - Server is backed up every 4 hours, retention for 1 week, plus 12 weekly archives.

- Encrypted password system - only you know your unencrypted password

- Password-protected downloads - files can be downloaded only by users who are logged in

- Files encrypted during upload and on server (maximum file size may apply)

In DETAIL:

Features	Description
Data protection during file transfer	
File transfer	Global Lounge employs SSL/TLS protocols to protect client authentication, authorization and file transfers.
High-grade encryption	Global Lounge secures files in transit with no less than 128-bit encryption using industry-standard encryption protocols.
File integrity	Global Lounge employs a keyed hashed message authentication code (HMAC) to authenticate and ensure the integrity of intra-system communications. Global Lounge verifies file size and file hash to ensure integrity.
Link generation	Global Lounge download links are uniquely and randomly generated using strong hash-based message authentication codes. Global Lounge provides technical countermeasures to protect links from guessing attacks.
Configurable settings	
Password policy	Clients have the option of configuring password policies, including password history, expiration, and complexity controls such as length, uppercase and lowercase letters, at least one number, and at least one special character
Custom SMTP (mail) settings	Global Lounge enables clients to route email messages though their own mail servers. When enabled, all emails sent through Global Lounge will be routed through the client's mail server, instead of Global Lounge mail servers. Clients may optionally configure the connection to support SSL.
Multi-factor authentication	Clients may set up a multi-factor (or strong) authentication process that requires submission of the account password and a secondary authentication, such as Google Authenticator or SMS/text message, in order to access the account. Global Lounge supports various two-factor and two-step authentication methods including forms and token-based authentication as well as SMS, voice and backup codes.

File retention	Users can choose to automatically delete files a certain number of days after upload to support retention preferences and policies.
Terms and conditions	Terms and conditions can be displayed on the login page, with the option of including a check box on the login screen that must be marked to indicate compliance with the terms before logging in.
FTP/FTPS	By default, file transfers occur over HTTPS (Port 443). Optionally, clients can connect to Global Lounge using FTP or FTP over SSL (FTPS connection over port 990), an inherently more secure protocol than FTP. Users can connect to Global Lounge directly from an FTP/FTPS program, providing a way for users to upload or download files to or from a secure location while using existing FTP/FTPS programs.
Account lockout	Global Lounge can configure your account to lock for five minutes after five invalid logon attempts to prevent account tampering. This application control is an account preference that can be customized to meet individual compliance needs.
Email notifications	Users can have customized notifications sent in real time.