APOSTROPH GROUP

The Language Intelligence Company

Security White Paper

At Apostroph, security and confidentiality are paramount

Security White Paper

Security and confidentiality in system selection and IT decisions are top priorities at Apostroph. This is also true of the choice of tools we make available to our employees and freelancers. Furthermore, our employees are regularly screened in accordance with the Federal Government's Ordinance on Personnel Security Screening. We are ISO 27001 certified.

IT security at Apostroph Group is based on five cornerstones:

- Physical security
- Security at system level
- Security at application level
- Network security
- Regular training of users

The Apostroph IT environment is in line with the banking standard. Both internal users and freelancers work exclusively with a personal user account, and multi-factor authentication additionally supports the already high security standards with a complex password. Furthermore, before starting their collaboration with us, all freelancers must sign the General Terms and Conditions to confirm that they will adhere to the specifications described in detail therein.

Anyone who starts or stops working for the company must sign a comprehensive confidentiality agreement. And anyone starting to work for the company also has to provide an extract from the register of convictions which must not date back more than one month. Many of our employees have also been screened and cleared in accordance with Art. 11 of the Ordinance on Personnel Security Screening (PSSO).

When you provide us with documents, these will remain confidential at all times – when you send them to us, during translation and also after we send them back to you. Two different levels of confidentiality for the placing of an order determine the level of security used during processing:

Company

Founded in 1994
160 employees
100 languages
> 2,000 language professionals
> 5,000 clients

Advantages

- In-house linguists
- Internal team of developers
- The latest translation technologies
- Customised corporate solutions
- Expert advice

Security

100% discretion and maximum security for your confidential data thanks to data hosted in Switzerland and ISO 27001 certified processes.

Levels of confidentiality			
Level	**Description/classification of the document to be translated**	**Security requirements**	**Security measures**
1	Normal – generally accessible information	None	General access in electronic form, protection against unauthorised access
2	Confidential	High	Access only for a limited number of users or internal employees

Physical security

IT infrastructure

Apostroph's servers are located in Switzerland with data hosting in Switzerland. The server environment is set up in such a way that it is completely redundant. Data is backed up every day. These data backups are stored externally in a safe place. All clients automatically lock when inactive. In accordance with our Clear Desk Policy, employees lock their computers or shut them down when they leave their desk. And this is something that is monitored; any employee failing to comply with this regulation is given a formal written warning by his/her direct line manager. This is kept in his/her personnel file.

Security

All documents are only processed digitally in principle. If processing on paper (due to the requested service) is necessary, these are stored exclusively under lock and key.

We enforce the Clear Desk Policy. All print documents to be destroyed are kept in a lockable container and then disposed of professionally by a certified document destruction company. Visitors have to make an appointment before visiting and are only allowed to spend time in the designated areas of our premises if they are supervised by a member of staff. Visits are documented in accordance with ISO 27001.

Security at system level

Processes/systems

Apostroph uses APOS (Apostroph Order System) for order processing. All working processes are distributed, monitored and concluded with APOS. APOS is also used to manage rights of access to the various databases.

Access to confidential data is regulated using passwords which are only available to the relevant user group. Access rights can only be issued by the administrators.
This is how Apostroph ensures that every customer order is handled in a controlled, secure environment at all times.

Access

The e-mail system is also protected with a password.
The passwords must fulfil specific security criteria and be changed every three months. A corresponding system prompt is automated and mandatory.

Confidentiality

The confidentiality level is determined by the customer when the order is placed in myAPOSTROPH. All orders marked as confidential can only be viewed by the relevant person who entered the order and a superuser defined internally.

Encryption

At Apostroph, data is SSL-encrypted.

Further specific encryption is used when Apostroph has direct access to customer systems (e.g. CMS tools).

Security at application level

Applications used

The applications mainly used by customers, translators and Apostroph are:

- Encrypted Microsoft Access applications
- Encrypted Trados translation memories and terminology databases
- Encrypted web applications
- B2B HTTPS & FTP web services

Microsoft Access

APOS is a proprietary Apostroph development based on Microsoft .NET and Vue.js. It has a professional SQL database. The web-based applications myFREELANCE (on the translator side) and myAPOSTROPH (on the customer side) are used for data exchange and are SSL-encrypted. They are also based on .NET and Vue.js. APOS S safeguards the entire process and its traceability: which freelancer carries out which services, who is involved in the project and what each person is responsible for, text type of the document to be processed, which languages the text is to be translated into, what level of confidentiality the order has, the deadlines that have been specified etc. This information is maintained for each order.

Trados Studio

Trados Studio or, at the request of the customer, another CAT tool is used as part of the translation process. For this purpose, the document is divided into segments (generally sentences) which are stored in a translation memory and can then be re-accessed when new documents are translated. This guarantees consistency, faster delivery times as well as lower costs.

Access to the translation memory and terminology databases is enabled per customer and freelancer for each individual case. This is protected with a personal user name and password with SSL encryption.

B2B services

There are various services available for automatic data exchange:

- myAPOSTROPH (HTTPS) customer portal for uploading and downloading order files
- Apostroph REST API for system-to-system connections
- CMS connector (e.g. for Drupal)
- Integration of hot folders, either in the client's environment or in Apostroph's environment

HTTPS-based solution (myAPOSTROPH)

All methods are protected with HTTP basic authentication. User name and password have to be provided on every service call. Customers can view the status of their orders in myAPOSTROPH (in progress, delivered, billed). Translations can also be downloaded there later. They can also generate reports on their orders (CSV format – can be opened and processed in Excel).

Network security

Setup

All employees work with the Citrix server. This means that all applications and resources are hosted centrally and can be called up remotely. It also ensures that the employees can access the working environment and keep operations going in times of crisis (environmental disasters, epidemics). Hosting and software updates are handled uniformly and controlled centrally. Data is always exchanged in an encrypted form. Utilisation is checked permanently.

Emergency plans are in place. Exercises on what to do in such situations take place on a regular basis.

Protection

The Apostroph firewalls are constantly being updated in terms of state-of-the-art technologies and software versions. The latest security patches from Microsoft are always used on Apostroph's working devices and servers. Anti-virus and anti-spam software is also installed and e-mails are scanned. All employees are regularly trained on the dangers of as well as how to react in the case of phishing, virus and hacker attacks. Some websites are blocked in principle for security reasons.

Regular pen tests and simulated phishing attacks are regularly carried out.

Company

Apostroph Group is the leading language service provider in the DACH (Germany, Austria, Switzerland) region with a total of 10 sites across Switzerland and Germany. Today, more than 5,000 companies and institutions rely on Apostroph's expertise. With 160 employees, including 40 linguists, and over 2,000 certified specialist translators, Apostroph offers language services in all disciplines and 100 languages, providing all industries with products tailor-made for the local markets. Extensive experience in language technology and process digitalisation, as well as the targeted collaboration of man and machine are the core components ensuring the quality and efficiency of Apostroph's services.