

INFORMATION SECURITY POLICY

Revision 6

1 Objectives

- 1.1 To develop an Information Security Management System (ISMS) to meet the information security requirements laid down in ISO/IEC 27001:2022 which is a part of the Integrated Management System of 1-Stop Bulgaria and which is aligned with the policies and procedures under ISO 9001:2015, ISO 17100:2015 and ISO 18587:2017.
- 1.2 To define specific policies and procedures for implementation of information security measures for protection of the company assets.

2 Scope

- 2.1 This Policy covers all company assets. For handling of specific security aspects, separate policies and procedures provide adequate details.
- 2.2 This Policy provides guidelines for appropriate employee and contractor behavior to achieve compliance with the best security practices.

3 Responsibilities

3.1 General Manager:

- ☐ Provides the resources necessary for implementing the information security measures.
- ☐ Ensures that all interested parties shall be informed of their obligations regarding information security.

3.2 Quality Manager:

- ☐ Ensures that the ISMS is integrated as a part of the general Integrated Management System of 1-Stop Bulgaria and the ISMS documentation is aligned with the documented information of other standards.
- ☐ Organizes training regarding compliance with information security requirements laid down in this Policy.

3.3 Information Security Officer

- ☐ Ensures compliance with this policy and implements or supports the respective experts in implementation of all information security measures.

- ☐ Monitors the performance and effectiveness of information security measures and makes proposals for improvement as appropriate.

3.4 Project Managers:

- ☐ Ensure compliance of their teams with all applicable information security provisions and report any suspected breaches of security to the Information Security Officer.

4 References

- ☐ Quality Manual
- ☐ Remote Work Information Security Procedure
- ☐ IT Security Policy
- ☐ Physical Security Procedure
- ☐ Human Resource Management Procedure

5 Terms and definitions

ISMS – Information Security Management System as defined in ISO/IEC 27001 and adapted to the operations of 1-Stop Bulgaria.

GDPR – General Data Protection Regulation (Regulation (EC) 2016/679)

NDA – Non-disclosure agreement (also called ‘**confidentiality agreement**’).

Contractor: A linguist, or a Project Manager, or the Resource Manager who are approved by or belong to 1-Stop Global Group and who are outsourced to fulfil orders from 1-Stop Bulgaria.

Linguist: A translator, editor or proofreader who is outsourced to fulfil orders from 1-Stop Bulgaria.

Access Control Officer: A 1-Stop Bulgaria employee responsible for the access control function (performed as an additional function by the Web Designer) and some hardware and software functions.

F1: The translation management system (TMS) of 1-Stop Global Group used by 1-Stop Bulgaria.

6 Activities

6.1 General

- 6.1.1 The requirements and guidance provided here are not meant to impose restrictions contrary to the spirit of trust in 1-Stop Bulgaria but to protect the company's good name, its employees, contractors and clients from illegal or damaging actions by companies and individuals, either knowingly or unknowingly.
- 6.1.2 The Information Security Management System is an essential part of the Integrated Management system of 1-Stop Bulgaria which complements the company's compliance with the best quality practices according to ISO 9001 and the best translating practices according to ISO 17100 and ISO 18578.
- 6.1.3 This Policy summarizes the general principles and practices related to information security whereas topic-specific policies and procedures provide detailed requirements about compliance with the information security infrastructure, technical and organizational provisions.
- 6.1.4 This Policy and all other policies and procedures which belong to the ISMS are mandatory for 1-Stop Bulgaria employees. **They shall be implemented with the participation of the whole management team and they shall be imposed to the extent possible given the fact that all employees are home-based.**
- 6.1.5 To ensure the efficacy of ISMS policies and procedures, they shall be regularly reviewed, at least once a year, and upgraded as required.
- 6.1.6 The implementation of ISMS can be subject to independent review to ensure all aspects of compliance. 1-Stop Bulgaria has decided, for security reasons, to assign this job to external trusted auditors who can audit the ISMS at regular intervals or for a specific reason (e.g., in case of big change).
- 6.1.7 The 1-Stop Bulgaria contractors are bound to comply with the ISMS of the company via the Non-disclosure Agreements as they are not 1-Stop Bulgaria employees.
- 6.1.8 The Integrated Management System of 1-Stop Bulgaria includes operating procedures about all company activities, including the use of translation tools and company platforms.
- 6.1.9 **1-Stop Bulgaria employees do not use encryption but may use IT facilities (such as electronic signatures) based on encryption technology.**

6.2 Information security objectives.

- 6.2.1 1-Stop Bulgaria has defined two sets of information security objectives within its ISMS.
- 6.2.2 The first set of information security objectives refers to information content and information management and they are related to the core activity of 1-Stop Bulgaria. The information content created and made available to its clients by 1-Stop Bulgaria shall meet the key characteristics of availability, integrity and confidentiality.
- 6.2.3 The organization of 1-Stop Bulgaria core activity – written translation – meets the requirements of the recognized international translation standards: ISO 17100:2015 and ISO 18587:2017 for machine translation. Certification to both standards by a

reputable international certification body and the excellent reputation of the company is the best evidence of the quality of work which includes information security.

6.2.4 The second set of information security objectives are organizational in nature and they include the following:

- Certification to ISO/IEC 27001:2022.
- Ensuring zero security incidents caused by employees and contractors.
- Improvement of NDAs to expand the scope of information security requirements.
- Ensure higher information security awareness by employees and contractors via training and written materials.

6.3 **Information security assets**

6.4 **ISMS in project management**

6.4.1 All projects of 1-Stop Bulgaria are subject to compliance with the requirements for information security, both by company employees and by contractors.

6.4.2 Information security is an essential aspect of the operation of employees and contractors as laid down in the Remote Work Information Security Procedure, IT Security Policy and Physical Security Procedure.

6.4.3 These procedures provide requirements and guidance on every aspect of the operation of employees and contractors.

6.4.4 They raise the awareness of employees and contractors of the importance of information security and alert them to potential risks.

6.4.5 The company managers are continuously raising their competences in information security threats and prevention techniques by following specialized security forums where they can ask questions and share experience with experts worldwide.

6.5 **Acceptable use**

6.5.1 The ISMS specify the requirements for compliance with information security and may be considered as guidance for acceptable use.

6.5.2 Whenever an employee is confronted by a situation which is not defined in the Integrated Management System of 1-Stop Bulgaria, guidance can be requested from the respective Project Manager.

6.5.3 In consequence of such cases, the ISMS can be reviewed and upgraded to expand the its scope.

6.6 **Unacceptable use**

- 6.6.1 The list below covers activities which are prohibited for 1-Stop Bulgaria employees and any third parties which have access to company facilities. The list is not exhaustive but it is meant to outline the categories of activities which fall under “unacceptable use”.
- 6.6.2 Under no circumstances is a company employee authorized to engage in activities which violate the Bulgarian or any other applicable legislation while using 1-Stop Bulgaria resources. Law-abiding and ethical behavior is encouraged for all company employees.
- 6.6.3 Writing and deleting electronic content on the company computers and systems must comply with the procedures and instructions implemented in the company and with the specific assignments given to each employee. Commitment to the company's interests and common sense shall be the guiding principles in writing and deleting electronic content.
- 6.6.4 Uploading on the company's computers any electronic content which may be subject to copyright, and no active license for it is available, is strictly prohibited.
- 6.6.5 Blogging from company facilities in one's own name is prohibited as it may endanger the company's good name and lead to litigation.
- 6.6.6 Involvement in any public activities, irrespective of the access point (such as a home computer), including internet activities (e.g., on Facebook), shall be done in a manner that (a) complies with all confidentiality restrictions of the company, and (b) does not in any way tarnish the good name of the company in which the employee works.
- 6.6.7 Contractors are not allowed to retain information of completed projects: once the project is over, the information shall be deleted from the contractor/s computer.

7 RECORDS

	Name	Notes

Rev	6	Reviewed by	Peter Tonchev	Approved by	Yana Dinchiyska	Effective date	25.07.2024
-----	---	-------------	---------------	-------------	-----------------	----------------	------------