STÁTNÍ TISKÁRNA CENIN,
státní podnik

The Security Audit

1. Scope and content of the security audit

The security audit will take place as an entry, before the conclusion of the contract, and will subsequently be organized regularly at three-year intervals. If necessary (change of contractual conditions, changes in security systems or rules, change of building or building modifications, etc.), an extraordinary security audit may be requested and carried out outside the regular three-year interval.

The security audit will be performed by representatives of the STC (1-2 persons) and the participation of an employee responsible for security (security manager or a person authorized by them) is required on behalf of the supplier.

The security audit will be organized in two days with the following agenda:

- 1st Day - security policy, security documentation, risk management, business continuity management, ensuring security processes, inspection of the building,
- 2nd Day - completion of the inspection of the building and checking the settings of security processes, processing the minutes of the security audit, conclusion,

The supplier will be informed about the security audit at least **2 weeks in advance** in case of the entry security audit (contact person stated in the tender), and at least **30 days in advance** in case of the subsequent security audits.

The content of the security audit is set out in the following part, Supplier Check Log.

2. Supplier security check log

Date: …………..

Conducted by STC commission composed of:

- Name, surname, ID No …………..

- Name, surname, ID No …………..

Name of subject checked: …………..

Responsible person (security manager or another designated person): …………..

No	Security Area	Actual Findings	Assessment (yes/no)
01	A certification according to ISO 14298 or CWA 15374 Standard	…………..	yes☐/no ☐
02	A certification according to ISO/IEC 27001 Standard	…………..	yes☐/no☐
03	A security policy implementation (Risk assessment, Security Policy document, other security documents etc.)	…………..	yes☐/no☐
04	A protection of classified information according to national standards (A confirmation from the national safety authority)	…………..	yes☐/no☐
05	STC subcontractors using for order processing	…………..	yes☐/no☐
06	Signed a confidentiality agreement with its subcontractors (NDA – Non Disclosure Agreement for example)	…………..	yes☐/no☐
07	A regular internal security audit performed on site once a year	…………..	yes☐/no☐
08	A risk management implementation	…………..	yes☐/no☐
09	An ability to deliver the product/service – Business Continuity management implementation, Emergency plans etc.	…………..	yes☐/no☐
10	Security requirements between STC and the supplier are set up and documented	…………..	yes☐/no☐
11	Outside CCTV cameras installed and connected to The Control Room, pictures are recorded and stored	…………..	yes☐/no☐
12	Inside CCTV cameras installed (in production area especially), pictures are recorded and stored	…………..	yes☐/no☐
13	An intrusion detection system (IDS) installed and connected to The Control Room and/or to The Police	…………..	yes☐/no☐
14	A Fire system installed and connected to The Control Room	…………..	yes☐/no☐
15	An Access control system installed, in production area especially	…………..	yes☐/no☐
16	A perimeter protection of the site (a fence, CCTV cameras, IDS)	…………..	yes☐/no☐
17	A mechanical protection to the production areas (turnstiles, walls, doors, bars…etc.)	…………..	yes☐/no☐
18	A space for loading and unloading of goods and materials is designated and monitored by CCTV	…………..	yes☐ /no☐

No	Security Area	Actual Findings	Assessment (yes/no)
19	A security guarding is performed by own employees or licensed outsourced guards	………….	yes☐/no☐
20	A key management is implemented	………….	yes☐/no☐
21	A production information system (data) is separate from public network and data are safely storage	………….	yes☐/no☐
22	The supplier employs own IT specialists	………….	yes☐/no☐
23	The supplier provides a policy for circulation and evidence of documents (Documents Management System e.g.)	………….	yes☐/no☐
24	The supplier possess policies for access to information systems during and at termination of employment	………….	yes☐/no☐
25	The supplier employs own staff for processing STC orders	………….	yes☐/no☐
26	STC products are separately and secured stored in the vaults	………….	yes☐/no☐
27	STC products are safely transported (GPS monitoring e.g.)	………….	yes☐/no☐

Issued certificates:

No.	Certificate	Certificate No.	Certificate valid till
01	ISO 14298 or CWA 15374	………….	………….
02	ISO/IEC 27001	………….	………….
03	Number and expiry date of the confirmation from the national safety authority	………….	………….
	………….	………….	………….
	………….	………….	………….

Additional information:

………….

…………………………………….   …………………………………….

…………………………………….