Date of last update	08.04.2022
Prepared by	Marcin Placek
Approved by	Zdenek Capek

Clause: ISO 27001:2013 - A.7.2.2 A.11.2.6, A.13.2.2,A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	GDPR Article: 5, 24, 25, 30, 28, 32, 1(3), 44, 45, 46,47, 49 ,82

Objective

Purpose of this policy is to define the way for Tristone and its Suppliers for handling Information security aspects during the business relation and beyond.
Specifically the objective of this policy is to secure Tristone's Information during:

a) Access and processing by third parties either at Tristone's Information processing facilities or at Third Party's location.
b) Outsourcing of services to third parties.

Scope

The scope of the policy applies to third parties including but not limited to vendors, service providers, system integrators who provide Information Technology (IT), Information Security (IS), IT Enabled Services (ITES) to Tristone.
[The term "third party" is generally referred as "vendor" throughout the policy for easy understanding].

Confidential information

Confidential Information means non-public confidential and/or proprietary information that it's owner designates as being confidential, howsoever recorded or preserved, or which should be reasonably known to the recipient to be confidential and/or proprietary in nature. Confidential Information includes, without limitation, information relating to owner's past, current and future products. It includes trade secrets, product plans, technology, research and developments, specifications for any products or parts, finances, computer systems, screens, market researches, marketing strategies, business plans, strategies or practices, designs, plans, drawings, data, algorithms, laboratories, prototypes, discoveries, methods, processes, procedures, improvements, "know-how," compilations, supplier relationships, customer names and other information related to customers, price lists, pricing policies and other information and materials from Tristone or any other party. This information is usually being used during a RFQ process or a project. The Confidential Information shall include all of the preceding information whether disclosed in written, oral, demonstrative, graphic, electronic or machine readable from or by any other media, directly or indirectly. The confidentiality applies before and/or after the Effective Date of a Non-disclosure agreement or start of the RFQ/project.
Confidential information includes **personal data.**

Requirements

All Confidential Information:

- shall be safely and securely kept and stored by the vendor. Vendor shall protect the Confidential Information with the same degree of care as vendor uses with its own Confidential Information (but in no event with less than reasonable care) in order to prevent the express, inadvertent or accidental disclosure of the Confidential Information and shall limit the reproduction and disclosure of such Confidential Information to its employees or directors to a strict need-to-know basis.

- shall not be disclosed to third Parties without the express written prior authorization of Tristone. If the Confidential Information is requested by a public authority as required by an applicable law or regulation (to the extent permitted by such laws or regulations), vendor shall give prompt notice of such request to Tristone (including by e-mail, the receipt of which is acknowledged) in order to permit Tristone to seek an appropriate limitation or remedy prior to such disclosure.

- shall only be used by vendor in direct relation with the purpose of the cooperation with Tristone.

Information Confidentiality protection

- Vendor shall sign a non-disclosure agreement with Tristone on maintaining the confidentiality of the above-mentioned Confidential Information; this means especially Tristone's or Tristone's customer specific information or personally identifiable information of employees of Tristone or Tristone's customer (which Vendor may have access to by virtue of working with Tristone) from unauthorized disclosures to third parties, without Tristone 's written consent.
- Non-Disclosure agreements executed between Tristone and Vendor shall be in accordance with Tristone 's approved NDA template.
- Vendor shall take all possible precautionary measures for maintaining confidentiality of data accessed from Tristone or otherwise.
- Vendor shall not disclose or misuse Tristone's details (such as services provided) without Tristone's written consent even for promotional activities including but not limited to sales, trade shows, campaigns, presentations and case studies.
- Vendor staff deputed at Tristone's premises for supporting Tristone shall not engage in disclosing Tristone's Confidential Information (especially Proprietary information) which they could have gained by virtue of their presence at Tristone.
- Documents created by vendor related to business engagement with Tristone shall be classified by vendor depending on the sensitivity of the document and as per the Information Classification Policy of Tristone.
- The access to information by the vendor shall be on need-to-know basis; Access shall be tracked and audited on periodic basis.

Information Security and Awareness

- Vendor staff working for Tristone shall understand Tristone's Information Security Polices.
- All vendor Staff (Full time Employees, Contractors) shall be made aware of the impact resulting from misconfiguration or human errors by service provider.

Compliance and Regulatory

- Vendor shall access Tristone's Applications & the IT systems based on the requirements and only for the intended purpose. Any misuse of privileges by the vendor or its resources on IT systems/Applications shall be treated as non-compliance to Tristone's Information Security policies and may attract civil/criminal liabilities.
- Summary of Third party compliance check on vendor's infrastructure shall be provided by Vendor to Tristone annually to assure Tristone on the Vendor's security controls implementation.
- Vendor assessments (due diligence and on ongoing basis) shall be conducted as required by Tristone's customer.

- Vendor shall comply with all the relevant regulatory and legal requirements.

Vendor audit

- Vendors who have an impact on Tristone's information security and Tristone labels them as such suppliers (even during cooperation), may be required to submit their information security policies (eg according to ISO 27001, etc.) to verify compliance with security rules.
- Such vendor should prepared at least the following documents:
  - security policy
  - risk analysis
  - disaster recovery related to the services provided
  - a protocol that his employees are regularly trained on information security
- At the same time, Tristone reserves the right to audit such suppliers. Tristone will let the supplier know about such an audit at least one month in advance. Both parties bear their costs for the audit. This audit can be replaced by a security questionnaire issued by Tristone and filled out by vendor.

Risk Management

- Tristone shall conduct information security risk assessment to identify various risks (related to People, Process and Technology) and review remediation plans before availing critical services from vendors. Critical services are services that demand stringent confidentiality, integrity, availability and privacy
- Identified control objectives and controls for the vendor, shall be documented and signed as part of the contractual agreement between Tristone and the vendor.
- Tristone and Vendor shall jointly review the identified risks and Non-Disclosure Agreements based on any changes in Business/IT environment.
- Security & privacy requirements shall be considered while choosing a vendor and if required, vendors shall be audited for their security & privacy practices.
- Access to applications hosted in Tristone backbone to third parties shall be provisioned through proxy.

Security Incident Management

- Vendor shall notify any type of security violation or security incident which may potentially affect Tristone's computing environment within mutually agreed timeframe

Operations/Administrative/Physical

- Tristone shall sign off Service Level Agreement (SLA) with the vendor for providing required support or service.
- Tristone shall review the SLA response at least on a quarterly basis.
- Vendor shall ensure physical & logical security of the vendor's equipment or Tristone's equipment managed by vendor (Inside and Outside of Tristone Premises) against intrusions, Denial of Service, and unauthorized access.
- Tristone reserves the right to monitor and audit the Applications, IT Systems and access between Tristone & Vendor.
- Tristone and Vendor shall mutually agree on the roles and responsibilities. This shall be documented and kept by both the parties for reference.
- Vendor shall comply with the same including pre-venting misuse of vendor privileged access/accounts provided to Vendor by Tristone for the purpose of troubleshooting, ongoing support and services.
- Vendor personnel shall be able to access Tristone's IT systems only after authenticating the identified individuals from Vendor side.

- Vendor shall be solely responsible for the misuse of account/access credentials made known to them as part of the business engagement.
- Movement of Vendor's resource deputed in Tristone shall be notified to Tristone immediately.
- Authentication, access rights and accounting details shall be reviewed during any vendor staff movement.
- Vendor staff deputed in Tristone shall be subject to Background verification check.
- Vendor shall follow documented change management process (Impact analysis, Review of changes, Roll back plan, approval mechanism, Communication inclusive) for all critical changes impacting Tristone.

Business Continuity and Disaster Recovery

- Vendor shall have documented recovery procedures for the services provided to Tristone as per service level agreement with Tristone.
- SLA shall be defined in the vendor contract to support Tristone and Tristone's customer's Business Continuity Plan (BCP) requirement.

April 2022

Marcin Placek
SVP Purchasing

Zdenek Capek
ISO

History of revisions

revision	changes to former release	author	date
1.0	Initial release	Marcin Placek	4.4.2022