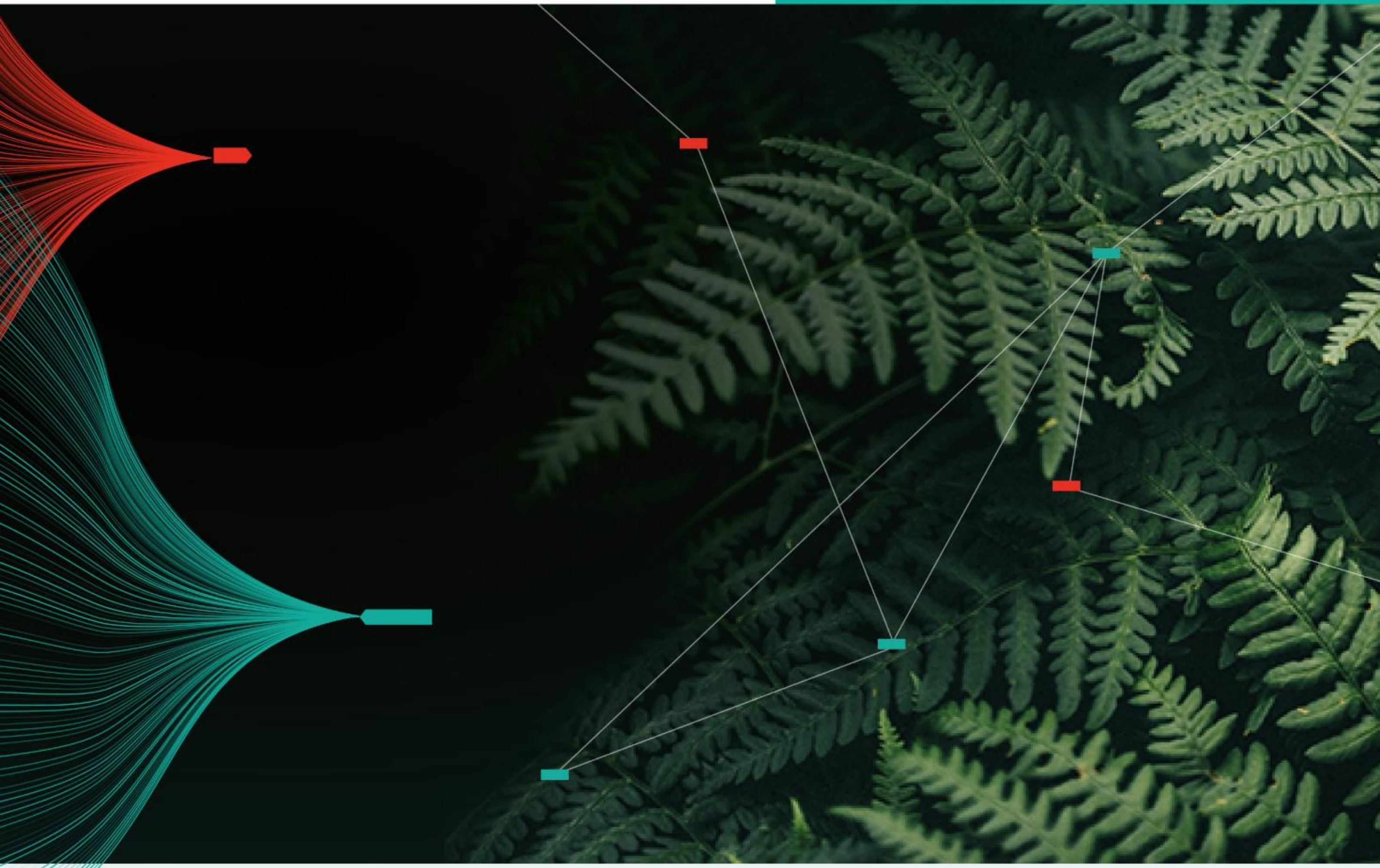
TARANDM

Decision Management, Big Data Architecture & Advanced Data Analytics

www.tarandm.com



Information Security Management System

	Information Security Management System
Author	Hana Valuskova, Office Management Team Lead
Version	v1.0
Date of issue	6.12.2023
Date of approving	6.12.2023

Table of Contents

1. Purpose

This document establishes our company’s Information Security Management System (ISMS).

The policies and procedures in this document have been prepared in accordance with the requirements of ISO/IEC 27001.

2. Company overview

Taran is a software company founded in 2019. We provide software products and related services in decision management, big data architecture and advanced data analytics. We are headquartered in Singapore and have offices and teams in Southeast Asia, Europe and North America.

Our flagship product TaranDM is a decision management platform, which helps our clients automate and improve their data-driven decisions. Our clients are mostly banks, fintechs and other financial institutions, but we cater to other industries as well.

3. Organizational goals and objectives

We set goals in IT security management area for every calendar year during the last quarter of the preceding calendar year.

For the year of 2024, we have set up the following goals and objectives:

- Perform regular application penetration testing (re-test)
- Make Security and Vulnerability scan audit results of Docker containers with our TaranDM application available to clients
- Further improve coverage of end-to-end automated application tests to achieve best customer experience
- Unify security and application logs into one logging instance
- Extend automated backup tools to cover multiple locations / various cloud providers
- Continuously self-educate ourselves & remain up-to-date with the latest trends in IT security

4. Used abbreviations and terms

- **An asset**: anything that has value to the organization in terms of information security
- **Availability**: ensuring that information is accessible to authorized users when needed
- **CEO**: Chief Executive Officer/company director
- **Collaborator**: means (i) an employee of the Company, regardless of the type of employment relationship and the size of the time commitment; (ii) a member of the Company's statutory body; and (iii) a natural or legal person who performs activities for the Company under a relationship other than an employment relationship
- **Company**: Taran Advisory PTE LTD, established under the laws of the Republic of Singapore, with registered address at 9 Raffles Place, Republic Plaza, #06-01, Singapore, 048619

- **Confidentiality**: ensuring that information is accessible or communicated only to those who are authorized to do so
- **CTO**: Chief Technology Officer
- **Integrity**: ensuring the accuracy and completeness of information
- **IS**: information security
- **ISMS**: information security management system
- **RP**: responsible personnel

5. Criteria for information classification

5.1. Protected information

Classification level II (restricted information) includes information which, from the point of view of confidentiality, is intended only for authorized collaborators of the company and authorized contractual third parties.

Protected information includes, but is not limited to, the following categories of data:

- personnel records of individual collaborators
- strategic documents that are accessible only to the company's management
- any personal or sensitive data belonging to company's clients
- any other personal and sensitive data in the sense of Regulation (EU) 2016/679 of the European Parliament and of the Council, On the protection of personal data, as amended (GDPR)
- any data that can be considered a trade secret

5.2. Unprotected information

Classification level I (unprotected information) includes information that is not restricted in terms of confidentiality. The information included in this classification level is intended for all collaborators of the company or public.

All promotional and marketing materials, descriptions of services offered, website content are publicly available.

6. Rules for handling information

6.1. Rules for handling unprotected information (classification level I)

Unprotected information is not subject to confidentiality. The collaborator of the company should abide with the following rules when providing such information:

- when passing information to another entity or when using information as a source for creating other derived information, the collaborator is obliged to verify whether the information is in the current version.
- a change in the content of publicly presented information (for example, a web presentation) is subject to a change procedure.
- communication in relation to the public (media, etc.) is provided by the company's management

6.2. Rules for handling protected information (classification level II)

The collaborator of the company should abide with the following rules when providing such information:

- when passing information to another entity or when using information as a source for creating other derived information, the employee is obliged to verify whether the information is in the current version.
- it shall be ensured by the collaborator during the transfer of information that the information will be available only to authorized recipients.
- the provision of information to third parties is only possible under the conditions that the third party has concluded appropriate confidentiality agreements with the company (on information protection) and the collaborator is entitled to provide information to a third party in the performance of his or her job function.

6.2.1. Specifics of written communication

- protected information may not be displayed on notice boards.
- protected documents must be printed on local printers or on printers where access to the documents by unauthorized persons will be prevented.
- the transfer of protected information to a third party through an intermediary must be securely ensured. The documents must be handed over to the intermediary in an opaque envelope and must be sent by registered mail.
- written documentation must be kept in lockable cabinets or in rooms with exclusive access by authorized persons.

6.2.2. Specifics of electronic communication

- when transmitting information by e-mail, the collaborator must verify that the recipient's e-mail address is valid and must use encryption when sending protected information.
- when transmitting information in the form of an electronic file stored on a data carrier, the collaborator shall ensure that the data carrier contains only information that is relevant to the given situation and at the same time only data with which the recipient is entitled to become acquainted. The data carrier must be protected against misuse of information by unauthorized persons by appropriate means.

- When transmitting information via the online electronic communication (chat, etc.), the collaborator must only use encryption when sending protected information.

6.2.3. Specifics of personal oral communication

- When transmitting information via oral communication, the collaborator must minimize the possibility of eavesdropping on the communication by a person who is not authorized to become acquainted with the protected information.

6.2.4. Specifics of remote oral communication

- in the case of remote oral communication conducted in the form of technical means without image transmission, the collaborator is obliged to make sure that the person he/she is talking to is the person he/she intended to talk to.
- the collaborator is also obliged to ensure that a third party cannot enter into communication between him/her and the recipient of the information if this is possible due to the nature of the technical means by which the communication is conducted.

6.2.5. Disposal of media with protected information

Safe disposal methods must be established for the disposal of media that contain protected information.

Every collaborator who comes into contact with protected information stored on the media is obliged to ensure their safe disposal. Such media usually includes, but are not limited to:

- internal/external computer hard drives
- flash memory modules (internal flash memory, USB flash memory, etc.)
- paper documents

Media that is not intended for shredding in a shredder and contains protected information must be safely deleted.

6.2.6. Safe media disposal means

- shredding: paper documents, CDs, DVDs, etc. must be shredded in a shredder
- physical destruction: defective computer hard drives, defective flash memory modules must be physically destroyed if they contain protected information

6.2.7. Transport of media with protected information

When transporting or transferring a media with protected information, the collaborator must ensure that the media is not left unattended (e.g. in a car).

Devices containing protected information that technically allow it must be also protected by suitable encryption tools.

6.2.8. Responsibility for determining classification

The classification of the relevant information asset is performed by the company management or by the Office Manager Team Lead.

6.2.9. Contact groups

- Company management: Eva Sobkova, Martin Chudoba, Vaclav Kozmik
- Contact with governmental and other public authorities: Martin Chudoba, Vaclav Kozmik, Hana Valuskova
- Contact with technical suppliers/vendors: Jan Šiftař, David Kubec
- Contact with clients: Martin Chudoba
- Internal communication: Hana Valuskova

7. Rules for using IT

7.1. Use of computer technology

Each collaborator must comply with Access Control Policy (lock screen, user password, security for sharing devices, clean tables and clear screen policy, password management, etc.).

If the collaborator has been provided with any computer technology from the company, he or she must hand it over when the relationship between the collaborator and the company is terminated.

7.2. Access to the system

All collaborators can access the electronically kept records only with the access credentials provided by the company and on the basis of the assigned access rights.

7.3. Using the system

Any technology provided by the company (Office365 email, OneDrive, SharePoint, Teams, …) should be used strictly for work purposes only. Collaborators cannot use it for any form of private business or matters.

No company information can be stored outside of the company’s controlled systems.

7.4. Using Email

When working with e-mail, each collaborator must pay increased attention to the delivered mail with an attachment. If a collaborator receives mail with an attachment from untrusted senders, they are not allowed to open or run the attachments; they are required to delete them instead. In case of any doubts, it is the collaborator's responsibility to contact the DevOps Team Lead. The collaborator must not engage in any illegal activities.

At the same time, a collaborator cannot forward to other collaborators any offensive, meaningless or misleading e-mails they have received from other collaborators or from an external network.

Incoming mail that is no longer needed for the collaborator should be deleted regularly (including deleting deleted mail from the folder). Information classified as protected can be sent via e-mail only in compliance with the rules defined throughout this document.

7.5. Hardware handling

If a collaborator has been given a hardware resource from the company, he or she is forbidden to manipulate it in any way without the consent of the DevOps Team Lead. It is strictly forbidden to perform any hardware interventions on the entrusted devices (for example, change computer components, connect your own external devices, etc.).

7.6. Software installation

If a collaborator is using a hardware resource from the company, he or she can install and use only legal software approved for use in the company.

7.7. Physical security rules

Each collaborator is obliged to ensure the protection of IT assets so that they cannot be misused by another collaborator or a foreign unauthorized person present at the workplace or elsewhere. This obligation might include:

- safe storage of the company's or collaborator's assets, for example in lockable room or box
- automated activation of a password-protected screen saver whenever the collaborator moves away from the workstation
- observance of the clean table rule, i.e.. do not leave loose documents classified as protected or data media containing information classified as protected on the desk or in public during their absence.

The work in the company's systems should be performed by the collaborator only for the time strictly necessary, and after the end or interruption of work, the collaborator is obliged to close the application in order to avoid the loss or damage of data. Before shutting down the workstation, the collaborator is obliged to properly close all running applications and log off.

7.8. Use of mobile devices

The collaborators are obliged to take extra care when using the mobile device for work purposes due to the possibility of theft of the device. It is forbidden to leave mobile devices in places where there is a risk of their theft or loss (e.g. in parked cars, in the trunk of a bus or plane, in areas without access control). Laptops and mobile phones must be password protected, in the case of storing protected data, it is necessary to configure and use hard drive encryption. Important data stored on mobile devices must be backed up. Theft of the mobile device must be reported immediately to the DevOps Team Lead.

7.9. Reporting failures, security incidents, vulnerabilities and emergencies

A security incident is an event in which information security fails or is intentionally or unintentionally compromised. Vulnerability is a weakness of the system (assets) that can be exploited by a threat. The collaborator is obliged to immediately report any security incident or vulnerability via internal chat tools, email or phone to DevOps Team Lead. The aim is to ensure an immediate resolution of the incident and an effective defense against its consequences. The collaborator must immediately report the fault and other detected defects on the workstation and other technical devices to the given message, especially if they could compromise security.

7.10. Antivirus protection, virus occurrence

The collaborators are prohibited from changing settings or disabling their anti-virus protection in any way. In the event of unknown or incomprehensible phenomena (e.g. on the display), the collaborator is obliged to immediately interrupt the work and report this fact to the DevOps team member. DevOps team member writes a record of this fact in the list of incidents if this case would be classified as incident.

7.11. Antispam protection

If spam messages are detected, the collaborator is obliged to remove them immediately and in the event of their mass occurrence (tens per day), he will report this fact via email to the DevOps Team Lead.

7.12. Regular back up

Collaborators are required to store and back up important data regularly.

8. Physical security

8.1. Physical access to buildings, office locations, security

The access to any company’s office, building, space or other premises should be on a restricted basis.

8.2. Key policy management

The key policy is maintained through a record.

This record contains:

- an overview of the authorized collaborators who are allowed to access the area
- date of handing over the key to the authorized collaborator
- the date of return of the key by the authorized collaborator

The management of the key policy implements and the individual measures are approved by the Office Manager Team Lead.

8.3. Check when leaving the room

A collaborator leaving a room in which other collaborators are no longer present is obliged to close and lock all lockable boxes - cabinets, close windows and perform a physical inspection of the room (power off for appliances where constant power supply is not necessary or appropriate, power off lights, etc.). The collaborator must also follow the rules set out in the chapter Rules for users of IT systems regarding leaving the room in relation to IT assets.

8.4. Visits

Visits are admitted to the company's premises only if the visitor is accompanied by a company’s collaborator.

9. System administration

9.1. Creating and deleting user accounts

Creating and deleting user accounts is described in Password Management Policy.

9.2. Use of mobile devices and computing equipment

The company uses primarily the following IT resources:

- laptops (multifactor secure protection)
- computer stations (multifactor secure protection)
- servers (key/token protection)
- mobile phones (multifactor secure protection)
- remote network access (multifactor secure protection)

9.3. Acquisition and registration of computer technology (HW)

DevOps Team Lead is in charge of the purchase of new computer technology either physically or virtually using cloud providers.

9.4. Data backup

Backup means the creation of backup copies of data files changed since their previous backup on backup media. Depending on the nature of the backed-up files, the hard disks/SSD disks can be also used as archive media.

These backup copies are used to recover data in the event of their loss due to computer failure, improper file manipulation or other means.

The DevOps Team Lead is responsible for backing up the information systems.

Backups performance is described in BackUp Policy.

9.5. Security against malicious software

All servers and workstations must be protected against malicious software (viruses, spyware).

Updates to this software and virus database are performed automatically when Internet connectivity is available.

Spyware protection is handled simultaneously with anti-virus scanning.

Each station has protection, which scans running applications, communication over the Internet using a web browser and other tools, control of opened documents.

Remote resources like Office 365 and Cloud infrastructure are protected by mechanisms of third party provider.

9.6. Operator logs

The responsible personnel managing IT systems record non-standard states of these systems in operator logs or similar records.

9.7. Records and reporting of security incidents and vulnerabilities

Security incidents are recorded in the Issue Tracker of company’s main GitLab. These security incidents are recorded and handled by the DevOps Team Lead in coordination with the other teams or the CTO.

Security incidents are regularly evaluated by the DevOps Team Lead. If he / she assesses that the incidents are serious, he / she always prepares a written report summarizing essential information about the reported incidents and vulnerabilities so that lessons can be learned from these cases.

The overall evaluation is carried out as part of the ISMS review.

In case of security incidents involving personal data, the following procedures should be followed:

- The company shall report security incidents that may result in a risk to the rights and freedoms of data subjects to the supervisory authority itself or through the relevant controller. In cases where a security incident may result in a high risk to the rights and freedoms of data subjects, the Company shall also notify data subjects.
- If the collaborator becomes aware or suspects that such security incident has occurred, it must notify the responsible officer immediately, and within 12 hours at the latest.
- Upon notification of a security incident, the DevOps Team Lead and the relevant collaborator shall take the necessary steps to avert the risks associated with the security incident (e.g. remotely erase or encrypt the lost electronic device, restore deleted data from backup, etc.) and assess whether, despite the measures taken, the security incident may have resulted in a risk to the rights and freedoms of data subjects.
- In the event that a security incident is likely to have resulted in a risk to the rights and freedoms of data subjects, the DevOps Team Lead, with the assistance of the relevant collaborator, shall report the security incident to
    - within 24 hours to the controller if personal data processed by the company as processor has been affected by the security incident;
    - within 72 hours to the supervisory authority if personal data processed by the company as controller has been affected by the security incident.
- The DevOps Team Lead shall state the following in the notification to the controller or the supervisory authority:
    - a description of the nature of the security incident in question, including, if applicable, the categories and approximate number of data subjects and the approximate number of personal data records affected;
    - the name and contact details of the DevOps Team Lead or other contact person representing the company;
    - a description of the likely consequences of the security incident and the likely risks;
    - a description of the actions the company has taken or plans to take to address the security incident and any mitigating measures that may be taken to address the potential adverse effects of the security incident;
    - an indication of whether or not the security incident should be reported to data subjects and the rationale for that decision.
- Where the security incident is likely to have resulted in a high risk to the rights and freedoms of data subjects, or where the supervisory authority, the relevant controller or the company itself so decides, the DevOps Team Lead shall also notify the security incident to data subjects, unless notification would require disproportionate effort. Notification to data subjects must be made by the DevOps Team Lead in an understandable form and must include:
    - a description and nature of the security incident;
    - the name and contact details of the DevOps Team Lead or other contact person representing the company;
    - a description of the likely consequences of the security incident and the likely risks;
    - a description of the actions the company has taken or plans to take to address the security incident, including any mitigation measures.

- A record of any security incident, even if unreported, shall be made by the DevOps Team Lead and the collaborator. The record shall record significant facts relating to the security incident, including:
    - the nature of the security incident;
    - the identification of the data and data subjects concerned;
    - the risk assessment of the security incident, including its justification;
    - information as to whether the security incident has been reported to the supervisory authority, the relevant controller, the company and notified to data subjects, including, where applicable, a justification as to why the report or notification was not made.
- The collaborator shall comply with the above mentioned obligations even if the security incident compromises only confidential information that does not contain personal data. In the event of a security incident that compromises solely confidential information that does not contain personal data, the DevOps Team Lead shall promptly notify the company's management to determine further action, unless the DevOps Team Lead is a member of the company's management.

9.8. Management of technical vulnerabilities

The DevOps team monitors the information concerning the discovered technical vulnerabilities, evaluates each such information and adopts an adequate solution in the form of, for example, the installation of so-called security fix packs.

In the case of assessing the state of technical safety through the implementation of safety tests, this activity must be performed in accordance with the Control Against Malware Policy

9.9. Systems Department

Testing and other risky operations are performed in such a way that important production functions are not disrupted or their performance is not limited. Operations performed in this way are performed on logically or physically separate elements (different databases or computers). Sensitive or security-problematic applications or systems should be operated separately.

9.10. Using cryptography

Each collaborator or any third party which is authorized to exchange information marked with the level protected, is obliged to assess whether the transmission of information is appropriate to use cryptographic means. If cryptographic means have been used in the past to protect the transmission of a similar type of information, it is necessary to contact the DevOps team in this matter. If the collaborator does not know the history of the use of cryptographic means or is unable to assess the appropriateness of the use of cryptographic means, he or she contacts the DevOps Team Lead or CTO. The DevOps Team lead assesses the suitability of cryptographic tools and decides on their use.

10. Evaluation of security systems

10.1. Safety test plan

Tests are performed in case of system changes (implementation or changes of information systems). In these cases, it is necessary to verify that no other system vulnerabilities have occurred. Safety tests will be performed by an entity designated by the DevOps Team Lead or company's management (internal persons / external persons).

10.2. Subject of safety tests

The tests are performed in order to determine the state of technical security of the information systems in the company. The subject of the test is to determine the state of their technical security with regard to the existence of possible vulnerabilities resulting from incorrect configuration or outdated state of security patches (these are various fix packs, hotfixes, patches). Testing of subject could be performed by internal mechanisms and external penetration test.

The subject of these tests is the company's infrastructure. This usually involves detecting vulnerabilities in the following areas:

- mail systems
- web servers
- firewalls
- active network elements
- work stations / laptops
- databases
- applications

11. Third Party Services

11.1. Identification of risks arising grom third party access

Physical or logical third party access to the company's assets may not be permitted until all risks that may jeopardize those assets have been considered. The identified risks arising from third party access must be covered by appropriate measures. Third party access must be approved by the appropriate Team Lead or CTO (responsible for evaluating possible risks and proposing measures to reduce these risks) and there must be written evidence (contract).

11.2. Security requirements in the contract with third party

Contracts with third parties should include, where appropriate, the following requirements:

- general rules of information security
- a description of the services that will be made available to the third party
- a procedure ensuring the return or liquidation of information assets after the termination of the contractual relationship

- responsibility for asset protection
- liability arising from applicable legal standards
- the right to monitor and prohibit third party activities
- responsibility for installation and maintenance of hardware and software
- a clear and specified change management process
- a description of the verifiable performance criteria and how they are monitored
- target service level and unacceptable service level
- conditions for third party cooperation with subcontractors
- the right to audit contractual obligations also through an external organization
- security incident reporting system
- possible penalties for infringements

11.3. Outsourcing

The term outsourcing would include any contractual relationship, which has the task of transferring responsibility for a certain part of the functional area, usually not belonging to the main activity of the organization, to external sources. The main difference between a traditional supplier (third party) and outsourcing is complexity - the organization transfers all responsibility for the selected activity to an external supplier. The contract with the outsourcing company must include the requirements listed above, plus information:

- how the availability of services in the event of an accident will be ensured
- how the legal requirements for the operation of the systems will be met

11.4. Monitoring and evaluation of third party services and outsourcing

Any service that is provided to the company by contract by a third party or through outsourcing must be regularly evaluated. The evaluation must take place on the basis of the requirements specified in the contract and is carried out by the manager of the particular service or relationship or a person authorized by company management.

12. Personal Data

12.1. General principles for the processing of personal data by the company

- The company shall only process personal data if it has least one legal title for the processing
- The company maintains a summary of each legal title by processing activity in the records of processing activities
- The company shall only process personal data in a fair and transparent manner
- The company will only process personal data within the limits of the legitimate, explicit and specified purpose of the processing of personal data

- If personal data are processed by the company pursuant to a standard contractual clause entered into with the company, the company shall process the personal data in question in accordance with this guidance and within terms of the relevant standard contractual clause
- The purposes of the processing specified by the company, other controllers, generally binding regulations or agreed in the standard contractual clauses concluded with the company can be found in the current records of the processing activities
- The company shall only process personal data that are relevant to the purpose and scope of the processing of those personal data
- The company shall only process personal data that are accurate and reasonably current. The accuracy and timeliness of personal data shall be the responsibility of the collaborator carrying out the specific personal data processing activity

Change History

Issue	Description of Change	Change resp. person	Date of Issue

Document Owner and Approval

The Q&A Team Lead is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to all collaborators on Corporate OneDrive.