



<b>Form</b>		
<b>Guideline for external contracting parties</b>	Creation date <b>07.03.2023</b>	page <b>1 von 6</b>
<b>FB-T 10-07 eng</b>	Modification date	Version <b>0</b>

## content

1. Purpose.....	2
2. Scope of application.....	2
3. Implementation .....	3
4. Validity .....	3
5. General requirements .....	3
5.1. Organizational requirements .....	3
5.2. Personnel security.....	4
5.3. Physical and environmental security .....	4
5.4. Management of values .....	5
5.5. Dealing with information security incidents.....	5

<b>Form</b>		
<b>Guideline for external contracting parties</b>	Creation date <b>07.03.2023</b>	page <b>2 von 6</b>
<b>FB-T 10-07 eng</b>	Modification date	Version <b>0</b>

## 1. Purpose

The "Information Security Guide for Partner Companies" defines the information security regulations to be taken into account by partner companies in their area of responsibility for IT systems and applications and infrastructure provided and used by them.

Partner companies must observe and comply with applicable regulations.

This information security guide defines the information security rules that partner companies must comply with when handling information and IT devices (e.g. PCs, workstations, laptops, smartphones or tablet PCs).


The purpose of the information security guideline is to protect the confidentiality, integrity and availability of information as well as to protect the rights and interests of the client and all natural and legal persons who enter into a business relationship with the client and/or perform activities for the client.

CleanControlling GmbH has introduced an information classification system to assess information security. Each external party is assessed in terms of its confidentiality, integrity and availability, and further action has been defined according to the classification.

## 2. Scope of application

The action guideline applies to the partner companies of CleanControlling GmbH and CleanControlling Medical GmbH&Co.KG and is to be applied throughout the partner network for partners who provide services for the aforementioned companies on the basis of contractual regulations and to be elaborated through concrete organizational and technical regulations (e.g. IT regulations) in individual cases.

The requirements are to be forwarded by the supply partner to subcontractors.

<b>Form</b>		
<b>Guideline for external contracting parties</b>	Creation date <b>07.03.2023</b>	page <b>3 von 6</b>
<b>FB-T 10-07 eng</b>	Modification date	Version <b>0</b>

### 3. Implementation

The described rules are independently binding for the partner companies as soon as information classified as secret or confidential is made available by the client, CleanControlling GmbH and CleanControlling Medical GmbH&Co.KG.

Information that is not marked as such must be treated as "non-confidential".

If individual regulations cannot be implemented in the current situation (e.g. technical reasons), the following procedure must be followed:

- the circumstance must be reported to CleanControlling (Medical) GmbH
- in the individual case, everyone must behave in such a way as to come as close as possible to the actual aim and purpose of the regulation.

In case of compelling need, deviating exceptions can be approved in writing by CleanControlling (Medical) GmbH.

### 4. Validity

This guide is valid indefinitely and without limitation.


### 5. General requirements

#### 5.1. Organizational requirements

Regulations of CleanControlling (Medical) GmbH regarding the bringing of external IT devices onto the company premises or into security areas must be observed.

The use of data or software on IT systems or storage devices that are neither provided nor released by the client or service provider is not permitted.

Data may only be passed on to third parties in compliance with these guidelines and only with the written approval of the data owner. An existing

<b>Form</b>		
<b>Guideline for external contracting parties</b>	Creation date <b>07.03.2023</b>	page <b>4 von 6</b>
<b>FB-T 10-07 eng</b>	Modification date	Version <b>0</b>

non-disclosure agreement shall be deemed a written release for data sharing.

Employees of the service provider must be obligated by their management to maintain confidentiality in accordance with the existing confidentiality agreement between the client and the service provider. The Client shall be granted access to these agreements at any time.

If the Client's data is stored on mobile systems or IT devices, these must be encrypted using state-of-the-art hardware or software.

Before traveling abroad, the country-specific regulations on the use of security technologies (e.g. encryption) must be observed.

After the end of the contract, the client's data must be handed over to the client and must be deleted from the service provider's devices and storage media or stored securely in accordance with the current state of the art. Legal requirements (e.g. retention obligations) must be observed.


## **5.2. Personnel security**

If a user has a user ID that is no longer required or an access right to the client's data that is no longer required, this must be reported immediately by the respective user to a responsible office (e.g. system administrator). This will be followed by immediate blocking/deletion. In principle, the minimum principle is to be applied when granting privileges.

The devices (e.g. laptops) and data carriers or storage media provided in connection with a service contract must be returned to the client when the contract expires or when they are no longer required.

## **5.3. Physical and environmental security**

IT devices that store or process CleanControlling (Medical) GmbH data must be used in such a way that no unauthorized persons can view or access this data. Special care must be taken when using mobile systems.

<b>Form</b>		
<b>Guideline for external contracting parties</b>	Creation date <b>07.03.2023</b>	page <b>5 von 6</b>
<b>FB-T 10-07 eng</b>	Modification date	Version <b>0</b>

As a matter of principle, confidential and secret documents must never be left unattended in order to prevent unauthorized persons from viewing them.

#### **5.4. Management of values**

In the context of information security, three primary protection goals must be pursued:

- Confidentiality
- Availability
- Integrity

In case of ambiguous classification regarding confidentiality, this must be requested from the contractor. Information must be protected from unauthorized access throughout its lifecycle in accordance with the measures corresponding to its confidentiality classification.


Information may only be made accessible to an authorized group of persons for the purpose of the agreed activities and in compliance with the relevant regulations.

#### **5.5. Dealing with information security incidents**

Information security incidents (e.g. malfunctions occurring, violations of the information security regulations, loss of secret or confidential information) that affect data or systems of the customer must be reported immediately to the responsible office named below:

security@cleancontrolling.de

Depending on the nature of the incident, the information security officer of CleanControlling GmbH decides on the further course of action and on the offices to be notified or called in, e.g. offices responsible for specific areas, the human resources department, data protection officer, etc. The information security officer of CleanControlling GmbH decides on the further

<b>Form</b>		
<b>Guideline for external contracting parties</b>	Creation date <b>07.03.2023</b>	page <b>6 von 6</b>
<b>FB-T 10-07 eng</b>	Modification date	Version 0

course of action and on the offices to be notified or called in, depending on the nature of the incident. He initiates the necessary measures to limit the damage and to remedy the disturbance.