



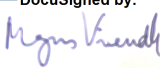
TriTiCon Policy

POL-05 IT and Data Handling Policy

Doc ID-Version POL-05 v1.0
Valid from 2024-04-10
Replaces Doc ID-Version New

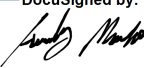
Issued by Magnus Värendh
Title Director

Date Signature
4/10/2024 | 13:01 CEST

DocuSigned by:

2C65CD72D9B6434...

Approved by Anders Mortin
Title Director

Date Signature
4/10/2024 | 04:56 PDT

DocuSigned by:

8BE4F7EC22BB467...



TriTiCon IT and Data Handling

TriTiCon are strongly committed to keeping all client and company information safe and secure. We operate according to the risk minimization principle, by which we strive to minimize handling, storage, and interchange of client information.

Contents

- 1. Objective 2
- 2. General statement 2
- 3. Key principles for IT environment and data handling 2

1. Objective

This Policy aims to ensure the establishment and maintenance of a safe and secure IT infrastructure to protect both client and company information at TriTiCon (TTC).

2. General statement

We operate according to the risk minimization principle, by which we strive to minimize handling, storage, and interchange of client information.

By this principle TriTiCon do preferably not handle or store clinical trial data or other data related to the clients' products. Should this be required in an assignment, the requirements and adequateness for technical solutions should be specifically assessed in the TMP-06 Client Engagement Checklist.

3. Key principles for IT environment and data handling

TriTiCon's IT environment for handling all client and company related information must comply with the following key principles:

Hardware and system security

All hardware and systems utilized at TriTiCon must be password-protected and maintained with up-to-date operating system security patches and malware protection measures. Adequate licensing for software is essential to ensure compliance.

Multi-factor and biometric authentication

If possible, implement multi-factor or biometric authentication to hardware and software.

User account management

User accounts must be personal and not shared under any circumstances to maintain accountability and prevent unauthorized access.

Data storage

Client and company information should primarily be stored on TriTiCon's secure Microsoft 365 OneDrive platform. Temporary storage on local drives for practical purposes such as traveling is permitted, but strict guidelines must be followed to ensure data security during transit and storage.

Access control

Access to client information should be granted on a need-to-know basis only, with no default access. This ensures that sensitive data is only accessible to authorized personnel, reducing the risk of unauthorized disclosure or misuse.

-

