# Security requirements and guidelines ESS R11 suite of data collection tools

***Version 1.0, September 2022***

## Introduction

This document provides security instructions for the organisations that will perform the ESS fieldwork with regard to the setup and installation of the SampleCTRL and the CaseCTRL application to conduct the ESS data collection. The instructions include a description of an obligatory minimum set of technical and organisational security measures that need to be taken and followed in order to ensure an appropriate level of protection of the processed data. Furthermore, recommendations regarding state of the art software and hardware to reach this aim are made.

All organisations conducting the ESS fieldwork are required to follow the instructions. Deviations from the following instructions may only be made after prior consultation of CentERdata and ESS HQ and have to be documented in writing. Such deviations will be accepted only if they do not lead to a reduction in the level of security and data protection.

## Webserver

1. Install the webserver software on a dedicated host. Only necessary services (web, administrator login) may be enabled on this host.
2. Access to the server via a remote service (Windows Remote Desktop or Linux SSH access shall be limited to the IT office workstations).
3. The webserver may only serve encrypted files via a secure way in order to ensure the secure transfer of data. One of the following three measures has to be applied:
    a. If possible, a VPN client shall be used to make the webserver only accessible via the virtual private network (in combination with firewall rules).
    b. Use the https protocol for the webserver to communicate between the CaseCTRL and SampleCTRL.
4. Limit the ability of webserver and web application user accounts to modify other programs, logs, or system configuration files by limiting account privileges.
5. Separate webserver content and related subdirectories from operating system and application directories.
6. The webserver shall be configured to prohibit access to files that may not be intended to be available for non-authenticated users. In particular, it has to be ensured that arbitrary directories are not made publicly available.
7. Keep discrete log files for each virtual webserver if there are multiple virtual webservers hosted on a single server instance.
8. Copy web service logs to a separate secure log server for retention.
9. Ensure mechanisms are in place to prevent log files from filling up the hard drive.
10. Perform regular backups (daily) of web content and occasional (minimal monthly) backups of operating system and application configurations.
11. Install an up-to-date professional antivirus software and perform regular virus scans.

## Database server

1. The database server needs to be on the same host as the webserver or on the same internal network.
2. The database may not be accessible by other hosts then the webserver.
3. If the database server hosts multiple applications, it has to be ensured that performance issues caused by other applications may not affect the Sample CTRL application.
4. It has to be ensured that access to the database is restricted to the application user and system administrator.
5. Databases have to be backed up on a daily basis.
    a. Storage of the backup files shall be offsite.
    b. The backups must be encrypted .
6. Backup and recovery procedures shall be periodically tested.
7. Key management procedures for decrypting backups have to be documented and must be available to more than one person.

## Client laptops and tablets

1. No private interviewer laptops or tablets may be used for fieldwork and shared use of interviewer laptops or tablets is not permitted.
2. Laptops and tablets have to be protected with a username and a secure password.
    a. It must be ensured that passwords are set in accordance with an appropriate global password policy.
3. When laptops or tablets are not used they shall be switched off and should be locked whenever possible.
4. The hard drives of the laptops or tablets need to be encrypted on an operating system level.
5. Keep operating systems up to date. In particular all security relevant updates shall be installed as early as possible.
6. A firewall needs to be installed on the laptops.
7. An up-to-date professional antivirus software has to be installed on all laptops and regular virus scans need to be performed.