## Purpose

Greenlight Guru strives to achieve a high degree of data and communication security as sensitive information may be stored in relation to the usage of Greenlight Guru Clinical. To ensure all stakeholders of Greenlight Guru that efforts have been implemented, this document clarifies which measures have been taken in design and production of Greenlight Guru Clinical - in relation to data-storage, -backup, -security, -privacy, and international and country-specific regulations which have to be complied with, when handling personal identifiable information or other sensitive healthcare related data

## Application

This document applies to all actors and users of the Greenlight Guru Clinical system as a whole. Greenlight Guru Clinical is owned, developed, and maintained by Greenlight Guru (SMART-TRIAL ApS, VAT NR: DK35139710). Greenlight Guru (SMART-TRIAL ApS) serves as an independent legal identity and is the copyright owner of Greenlight Guru Clinical.

All users of Greenlight Guru Clinical are direct customers of either Greenlight Guru or SMART-TRIAL ApS and shall therefore only be bound to usage, license, and data processing agreements with Greenlight Guru or SMART-TRIAL ApS.

Purpose
Application
References
Terms
Security Statement
1. Greenlight Guru Clinical Policies and Procedures
1.1. Information Security Management
1.2. Data Protection Officer
1.3. Human Resources and Education
1.4. Access Control
1.5. Production Monitoring
1.6. Design, Development, Verification and Validation Standards
1.7. Greenlight Guru Clinical Development Stack
1.8. Coding Standards
2. Hosting Services and Data Policy
2.1. Hosting Service Provider
2.2. Infrastructure - Microsoft Azure
2.3. Data Ownership and Limits to Data Sharing
2.4. No-Direct-Data Access Policy
2.5. Data Access in Case of Unforeseeable Events
2.6. Hosting Service Security Certificates and Standards

2.7. Greenlight Guru Clinical Data and Hosting Location
3. System Availability
3.1. Service Uptime
3.2. Service Downtime
3.3. Service Failure & Recovery Time Objective
3.4. Data Backup
3.5. Updates and Service Maintenance
3.6. Business Continuity and Disaster Recovery
4. Infrastructure Security
4.1. Threat Management
4.2. Network Connection
4.3. Segregation of Testing Environment
4.4. Logging, monitoring and reporting
4.5. Physical & Network Security
4.6. Technical and Contractual Safeguards to Protect Personal Data
5. Greenlight Guru Clinical Operation- and User-Security
5.1. Communication Encryption
5.2. General User Security
5.3. Two Step Verification and Authentication
5.4. User Password Standard
5.5. Login Brute Force Defence
5.6. Password Protection Policy
5.7. Access Logging
5.8. User Permissions and Roles
5.9. Greenlight Guru Clinical Administrative Staff Access
5.10. Encryption of Sensitive Data
5.11. Data Separation
5.12. Data Export
5.13. Audit- and Transaction-logging
5.14. Deletion of Data and Study Specific Logs
5.15. Supported Browser
6. Study Data Collection
7. Breach of Security
8. User's Responsibility
Are we Missing something?
Older versions

## References

1. https://azure.microsoft.com/en-us/support/trust-center/compliance/
2. https://azure.microsoft.com/en-us/support/legal/sla/summary/
3. https://azure.microsoft.com/en-us/support/trust-center/privacy/
4. https://azure.microsoft.com/en-us/support/trust-center/security/
5. https://azure.microsoft.com/en-us/support/trust-center/security/monitor-log-report/
6. http://www.datatilsynet.dk/Danish Data Protection Agency
7. Danish law order nr 528since 15/06/2000 with changes (nr 201 since 22/03/2001) - Sikkerhedsbekendtgørelsen
8. https://www.microsoft.com/en-us/TrustCenter/Privacy/Responding-to-govt-agency-requests-for-customer-data
9. https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/#locally-redundant-storage
10. https://azure.microsoft.com/en-us/regions/

## Terms

**May:** Used to describe a permissible way to achieve compliance
**PII:** Personal Identifiable Information
**Shall or must:** Compliance is mandatory
**Should:** Compliance is recommended, but not mandatory
**SOP:** Standard Operating Procedure
**User/customer:** Used to describe a person that has a user account in Greenlight Guru Clinical

## Security Statement

### 1. Greenlight Guru Clinical Policies and Procedures

#### 1.1. Information Security Management

We have a set of standard operation procedures (SOP) which state how information security shall be managed within Greenlight Guru Clinical. This covers not only general internal information security, but product specific information security as well, such as those regarding Greenlight Guru Clinical and Greenlight Guru Clinical customers.
The SOPs specify how all employees and subcontractors should conform with information security and data management at Greenlight Guru Clinical, and is certified under ISO27001 and ISO9001.

#### 1.2. Data Protection Officer

Greenlight Guru has appointed a Data Protection Officer who handles all data protection issues and queries regarding Greenlight Guru Clinical. This is required according to the EU regulation 2016/679. The data protection officer can be contacted via e-mail. Any enquiries regarding data protection, and data policy, will be handled and responded to in a timely manner, according to the specifics noted in the 2016/679 EU regulation.

### 1.3. Human Resources and Education

All personnel that have access to, or administrate production environments, which contain PII, are educated in the concepts of information security and relevant technologies, and must adhere to all relevant SOPs within Greenlight Guru Clinical. Only employees who have been certified by Greenlight Guru Clinical's managing director can gain access to perform administrative operations on production environments for Greenlight Guru Clinical (e.g. verifying backups).

### 1.4. Access Control

Access to any security critical systems of Greenlight Guru Clinical, such as databases management systems, servers, or other production environment technologies, are only provided to specific employees on a need-to-know basis. Access to each of these systems is handled in coherence with the internal information security management SOPs. A record of system access is kept for compliance purposes and reviewed accordingly

### 1.5. Production Monitoring

All production systems and servers are monitored for malicious activity and maintained accordingly – both manually and via automatic monitoring. Access logs to servers, and production service environments are reviewed on a regular basis

### 1.6. Design, Development, Verification and Validation Standards

Greenlight Guru's quality assurance is based on and in compliance with the PIC/S Guidance, PI-011-3 Good Practices for Computerized Systems in Regulated "GxP" Environments, and the software validation process is based on IEC 62304. Greenlight Guru Clinical simplifies regulatory compliance for ISO 14155 (GCP), FDA 21 CFR Part 11, GDPR, and HIPAA by offering ready-to-use QA templates, system modules, and guidance documents.

### 1.7. Greenlight Guru Clinical Development Stack

Greenlight Guru Clinical is primarily coded in JavaScript, HTML, CSS. Both application and database management systems run on combinations of Linux and Windows servers.

### 1.8. Coding Standards

Development and software programming is performed according to Greenlight Guru's quality management system standards. Code styles used are in coherence with Google's coding styles and all development follows specific workflow guidelines. All production code is subject to regular code inspection/review and testing

## 2. Hosting Services and Data Policy

### 2.1. Hosting Service Provider

Microsoft is the only hosting service provider for Greenlight Guru Clinical. Microsoft are bound by a GDPR compliant data processing agreement with Greenlight Guru (Microsoft Products and Services Data Protection Addendum) which includes the latest standard contractual clauses (SCCs) and prohibits Microsoft to provide any information or data in

relation to Greenlight Guru Clinical to third parties unless specifically authorized to do so[4][5].

### 2.2. Infrastructure - Microsoft Azure

All data, and production environments for Greenlight Guru Clinical are stored and hosted on Greenlight Guru's private and secure hosting services within Microsoft Azure. No third party has access to any data on Greenlight Guru's hosting services [5].

### 2.3. Data Ownership and Limits to Data Sharing

All data in relation to a specific study created within Greenlight Guru Clinical is owned by the study creator/owner and its participants. Data can be delivered in raw format to the study owner by request at any time. study creator/owner can export all relevant data from within the system using the available data export functions.
All other data stored with Microsoft Azure in relation to Greenlight Guru Clinical is owned by Greenlight Guru, and any government and law enforcement request to access data is performed in coherence with the appropriate legal process – see [4] and [5] for more details.

### 2.4. No-Direct-Data Access Policy

Greenlight Guru has designed Greenlight Guru Clinical to adhere to a "No-Direct-Data Access Policy". This means that Greenlight Guru Clinical cannot be used by Greenlight Guru's administrative staff to access customer data without direct permissions given from data-owners (study owners). In any case, a study owner is always responsible for giving out permission to those users who should be able to view/access their data, which can only be done via the platform itself.

### 2.5. Data Access in Case of Unforeseeable Events

As long as Greenlight Guru has legal ownership of Greenlight Guru Clinical and its production environments and hosting services Greenlight Guru Clinical customers shall be able to access their data via the Greenlight Guru Clinical platform. Only upon special requests can data be acquired directly from Greenlight Guru, i.e. if data cannot be acquired from Greenlight Guru Clinical directly.
Microsoft will never reveal any data directly to Greenlight Guru Clinical customers or other third parties [4][5] without explicit permission from Greenlight Guru, as long as Greenlight Guru is an established legal entity.

In the case of where Greenlight Guru is no longer an established legal identity, or a business organization of any sort which allows Greenlight Guru to maintain or withhold Greenlight Guru Clinical and its data as described within this statement and Greenlight Guru Clinical license agreements, the following procedures will unfold.

1. Greenlight Guru will release a formal notice to all Greenlight Guru Clinical users to inform them of the specific circumstances and why they have unfolded.
2. Greenlight Guru will ensure that all users will be able to receive a copy of all relevant study data, by either requiring all study owners to export them directly from Greenlight Guru Clinical, or by delivering raw data exports of each study to its legal data controller.

3. Greenlight Guru will ensure that any data stored within Greenlight Guru Clinical is not removed or deleted until all customers and data owners have been informed of these procedures.
4. SMART-TRIALApS will enable all Greenlight Guru Clinical customers to retrieve their data from Greenlight Guru Clinical within a specific period of time defined in the formal notice – from hereon called the "retrieval period".
5. After the specific retrieval period, Greenlight Guru will ensure that all data is safely deleted and after which will inform all customers of this operation. Thereby no PII data will be longer contained within any identity of Greenlight Guru or its hosting service providers, and thereby only with data owners.

However, these procedures do not unfold if another legal identity accepts, or overtakes the legal data responsibilities of Greenlight Guru in regards to Greenlight Guru Clinical, such as in the case of a merger and acquisition, and its customer's data – in this case, all Greenlight Guru Clinical customers will be informed beforehand.

### 2.6. Hosting Service Security Certificates and Standards

The Microsoft Azure platform itself and Microsoft data centers are certified with a broad set of international and industry-specific standards such as: ISO/IEC:27001, ISO/IEC:27018, FedRAMP, and SOC 1 and SOC 2. Microsoft Azure cloud services also meet regional and country-specific standards and contractual commitments, including the EU Model Clauses (i.e. EU Data Protection Directive 95/46/EC), UK G-Cloud. In addition, rigorous third-party audits, such as by the British Standards Institution and Deloitte, validate the adherence of the Azure cloud services to the strict requirements these standards mandate. The complete list of compliance standards, certificates, third party audit reports, and white papers for Microsoft Azure its datacenters can be found from [2].

### 2.7. Greenlight Guru Clinical Data and Hosting Location

All data in relation to Greenlight Guru Clinical is stored on secured Microsoft Azure hardware located in the European Union [11]. Due to security measures, and conformity regulations with international and country-specific standards, Microsoft does not disclose the details of a physical addresses to its data centers to any of its customers, including Greenlight Guru. Therefore, Greenlight Guru cannot, and will not, require Microsoft to disclose the physical location in more detail. However, Greenlight Guru and Microsoft Azure ensure that all data is stored using geo-redundant storage (GRS) where data is replicated synchronously three times in the primary region (Ireland) and also in a secondary region (the Netherlands).

Greenlight Guru highly values its customers' data privacy and security, and therefore highlights that information such as a physical street address or housing of data servers is non-relevant in this case of data privacy and security and will only be regarded as a security-risk if revealed.

Since SMART-TRIAL ApS (legal entity for Greenlight Guru Clinical in Denmark) is a legal identity within the kingdom of Denmark, Greenlight Guru must conform to Danish and EU legislation and regulations regarding data privacy and data processing. According to both the Danish data-protection agency (Datatilsynet) [7] and the Danish law order for security and protection of PII, which are handled by public legal identities

(sikkerhedsbekendtgørelsen) [8], it is NOT required by data processors, such as Greenlight Guru, to reveal more detailed information of a physical addresses of data service providers and data servers, other than country or city/state specifics.

It is therefore up to the data processor, to decide if customers are required to be informed of such information or not. If required by law, for any Greenlight Guru Clinical customer to access his data from a physical address, without having to acquire it via Greenlight Guru, Microsoft will accept law enforcement request to access customer data and will be handled as described in [5] and [9].

## 3. System Availability

### 3.1. Service Uptime

The services and interfaces of Greenlight Guru Clinical follow the hosting provider's availability and uptime guarantees. This means that all users of Greenlight Guru Clinical, apart from those located in Asian countries and Russia, can receive and process requests at minimum 99.9 % of the time (usually around 100%), as Microsoft Azure promises a server uptime of minimum 99.9 % per [3]. Greenlight Guru strives to keep uptime of all Greenlight Guru Clinical services as high as possible, and are notified continuously if any downtime is experienced. Uptime is defined as the amount of time the Greenlight Guru Clinical system is up and running and available for use. Uptime is measured per month, and is calculated from the following formula: % uptime each month = 100 x ((24 x number of days in the month) – total downtime in month) / (24 x number of days in the month).

### 3.2. Service Downtime

Downtime is defined as the number of hours the Greenlight Guru Clinical system is not up and running and available for use during one month. However, the following conditions do not represent the system being out of reach, and thus not included in the definition of downtime:

- Maintenance and migration at Greenlight Guru Clinical or its hosting provider
- Errors and crashes for any reason, that occurs on the user's own network, power- or IT-system, hardware, including system software, as well as lack of access to the user's network and an active internet connection
- Errors and crashes for any reason that occur because of an incompatibility between the user's IT system and the Greenlight Guru Clinical system, such as incompatible browsers. See 5.15 for a list of supported browsers.

Per definition, all service windows are included in the uptime guarantee, if notified at a minimum of 3 days in advance. In cases that are to be classified as emergencies, which require an extraordinary service window, services or maintenance windows are announced at least 24 hours in advance.

Emergency service windows are only announced in cases where security issues are discovered.

### 3.3. Service Failure & Recovery Time Objective

Greenlight Guru Clinical makes use of multiple services to serve/store data from users, such that if any service becomes unavailable, the system will be able to re-initiate operation without serious inconvenience, or loss of any data. Greenlight Guru Clinical utilizes a specific replica-set technology, to distribute data between secure servers that enables consistent and high availability of all data stored in Greenlight Guru Clinical.

If a server becomes unavailable, the Greenlight Guru Clinical personnel is immediately notified such that a resolution can be found as quickly as possible. Server failures should not affect performance of Greenlight Guru Clinical interfaces and users should in most cases not be affected by any server failures - see 3.1 and 3.2 In any case, Greenlight Guru Clinical personnel will strive to return all services back to normal within at least 24 hours

### 3.4. Data Backup

Backup of all data stored in databases is performed regularly such that data can be restored in case of any critical failures. Backup is performed by multiple machines, where data is continuously replicated multiple times 24/7/365. In addition, continuous file system backups are made on all data and stored separately. Backups have however a maximum lifetime of 14 days. Due to the fact that if any study data is requested to be deleted by a Greenlight Guru Clinical customer, backup data must be deleted as well. All backup data, and backup to any services used by Greenlight Guru Clinical is kept within the European Union as previous mentioned in 2.7 and documented and described by Microsoft in [10] and [11]. All data is backed up using geo-redundant-storage (GRS) using the primary region North Europe (Ireland) and secondary region West Europe (Netherlands)

### 3.5. Updates and Service Maintenance

For every new Greenlight Guru Clinical version release, all users of Greenlight Guru Clinical are informed, with information on changes and/or feature updates. In most cases, a version release should not affect users in critical ways. If such critical releases are required, all users will be informed of the specifics timely, to prepare for any inconvenience which they might experience.

### 3.6. Business Continuity and Disaster Recovery

Greenlight Guru has a policy and a plan in place which covers how business continuity and disaster recovery is handled. Greenlight Guru's management conducts testing and review of these objectives continuously, such as on re-location of workspace and communication channels, backup recovery and deployment of production environments.

## 4. Infrastructure Security

### 4.1. Threat Management

Microsoft Azure provides threat management in relation to services hosted by Azure, and as such Greenlight Guru Clinical and the underlying network used to link Greenlight Guru Clinical services together is subject to threat management as described in [5], hereunder techniques for DDoS prevention, intrusion detection, injection preventions, and anti-malware. Once a year Greenlight Guru hires an external security advisory company to conduct a penetration test on the Greenlight Guru Clinical platform and its infrastructure. Greenlight Guru Clinical customers can request a copy of the penetration test report.

### 4.2. Network Connection

The servers running Greenlight Guru Clinical services are locked on all ports except for the ones used by the system internally, and only accepts requests from the internal service IP addresses. The public web-interface servers only accepts connections on port 443 (HTTPS) and port 80 (HTTP), however access on HTTP will always redirect to HTTPS in order to ensure full network encryption between all services and Greenlight Guru Clinical customers and clients.

### 4.3. Segregation of Testing Environment

All new system functionality and design changes are verified and validated per Greenlight Guru SOP (system functionality and security testing) in a separate testing environment fully separated from the Greenlight Guru Clinical production environment before being made available to the public production environments.

### 4.4. Logging, monitoring and reporting

Access to any services hosted by Microsoft Azure is subject to audit logging [6] and as such all attempts to access any servers used Greenlight Guru Clinical are logged for security analysis and monitoring. Any server failure is automatically reported to the Greenlight Guru personnel as well.

### 4.5. Physical & Network Security

Greenlight Guru staff work from a physically secure location, where appropriate network and physical security measurements have been implemented to minimize security risks on production environments of Greenlight Guru Clinical. Greenlight Guru staff that have to interact with production environments use only computer equipment that has been certified by management to connect with any work environments. Physical location and network are reviewed by management on a continuous basis to minimize any vulnerability or unauthorized access. Access to a physical office location and/or internal office network, does not provide any access to product or testing environments of Greenlight Guru Clinical.

### 4.6. Technical and Contractual Safeguards to Protect Personal Data

Greenlight Guru Clinical implements both contractual and technical safeguards, as recommended by the EDPB (European Data Protection Board), to minimise unlawful access and processing of personal data, especially by third-country sub-processors. Additional technical safeguards include for example storage of encryption keys separately from application and data hosting services, using FIPS 140-2 Level 3 validated HSMs (Hardware Security Modules). Contractual safeguards include the use of the latest EU SCC and DPA template from the EU in Greenlight Guru Clinical's online data processing term and the use of EU SCC with our sub-processors, while also limiting access to personal data using industry best-practice access security and encryption mechanisms.

## 5. Greenlight Guru Clinical Operation- and User-Security

### 5.1. Communication Encryption

All communication between users of Greenlight Guru Clinical and the system is encrypted with use of the Secure Socket Layer (SSL) and Transport Layer Security (TLS) technologies, which ensures that ALL data sent between clients and the Greenlight Guru Clinical system is obscured from outside parties. Furthermore, SSL and TLS makes use of data encryption and server verification, which implies that data only can be interpreted by the intended parties.
The Greenlight Guru Clinical system is split into different entities to ensure availability. All communication between the internal entities of Greenlight Guru Clinical is performed via secure SSL/TLS connections as well, such that data may not be interpreted by third parties during internal system communication.
All encryption standard for Greenlight Guru Clinical, for both communication and data encryption, is at minimum AES-256 (i.e. the AES algorithm using 256 bit keys).

### 5.2. General User Security

To collect and view data, or access a study in Greenlight Guru Clinical users must create a user account with an associated strong password, which shall be used to authenticate with the system. Users shall provide the following information and accept usage terms before being able to authenticate against the system.

- Full Name
- Password
- Mobile number
- E-mail address

E-mail address is used as a unique identifier for user profiles, as well as username to login. Mobile number and password are used to validate authentication of each user profile. In addition to these information, the following are optional and can be required collaborators by SOP in individual studies.

- Organisation
- Staff ID
- Department
- Address (Street, Country, Zip etc.)

### 5.3. Two Step Verification and Authentication

To perform any security critical actions within the system, a user must be authenticated. Greenlight Guru Clinical implements two-step authentication for every log in, i.e. users must log in to the system using their created credentials and confirm their authentication with a unique one-time code sent to their mobile phone or e-mail address. In addition, user can also ask the system to call them directly for confirming the one-time code. On successful authentication, Greenlight Guru Clinical creates a unique user-session that is used to identify the authenticated user. The session contains no information about the user's password or other personal identifiable information and is valid for a limited time only. When the session expires, a user can choose to prolong his session by re-authenticating against the system - this is however only possible for 15 minutes. If a user does not prolong his session within this 15-minute time frame, the system

automatically disables the user session and logs him out of the system, requiring him to perform a complete two step authentication against the system.

Greenlight Guru Clinical does not accept any interface or data requests that do not have a valid session.

### 5.4. User Password Standard

Greenlight Guru Clinical requires user passwords to conform with a high level password security to limit the possibility of brute-force attacks. A user password is stored with individual salt values and hashed multiple times. Passwords cannot be recovered in clear text and do require users to create new passwords in case of a lost password. Greenlight Guru Clinical's password policy is strict, and every user must create a password that must consist of at least all of the following

- 8 Character Long
- One upper and one lower case character
- One number
- One special character

### 5.5. Login Brute Force Defence

Greenlight Guru Clinical is protected against user profile brute force attacks, by utilizing two-step verification as described in 5.3 "soft-lockout", and "hard lockout". "Soft-lockout" enables captcha verification to be performed after 3 unsuccessful login attempts and user profile "lockout" is activated after 5 unsuccessful login attempts. This requires a user to contact Greenlight Guru Clinical support directly for unlocking the user profile. All unsuccessful login attempts are logged – see 5.7

### 5.6. Password Protection Policy

Even though security measures are employed in regards to passwords, users are still responsible for defining their own secure passwords, and not sharing their passwords with anyone. Greenlight Guru recommends that individual organizations confirm with the ISO/IEC 27001 and 27002 standards for information security management. Greenlight Guru Clinical does not require users to change their passwords, but as a recommendation, they should be changed regularly for security measures.

### 5.7. Access Logging

All non-successful authentication and unauthorized requests tries, are logged within the system and only accessible by Greenlight Guru Clinical system administrators. These access logs are reviewed regularly as described in 1.4. If suspicious activity is noted, the specific user profiles will be analyzed in detail and the owner of the user profile will be contacted.

### 5.8. User Permissions and Roles

Greenlight Guru Clinical makes use of permission based access to every data created/collected in relation to studies. Only the owner of a study, and users that have been given explicit access by the study owner via the system, may gain access to the study's data. Each study owner is therefore solely responsible for keeping track of all collaborators (i.e. users that have been given any type of access to the study), their roles,

and permissions. All manipulation of user permissions to studies is logged in the study audit log (see 5.12).

**5.9. Greenlight Guru Clinical Administrative Staff Access**

Greenlight Guru Clinical administrator/support users have no access to any of the studies created within the system. Administrative users can therefore only gain access to a study and its data, if a study owner gives an administrative user profile explicit access to their study.

**5.10. Encryption of Sensitive Data**

Specific sensitive data attributes stored in relation to user profiles, subject profiles, and form answers are stored in an hashed format, and may only be decrypted with the corresponding encryption key and system specific methods. The encryption keys are stored securely and only available to the system internally and cannot be used by any administrative staff or other users solely to decrypt information in case of security breach – due to the “No-Direct-Access Data Policy” see 2.4.

**5.11. Data Separation**

Greenlight Guru Clinical stores study specific data in separate databases, such that all data for individual studies are clearly separated. Each study database is fully encrypted and only accessible by the study owner/creator via Greenlight Guru Clinical and the Greenlight Guru Clinical system internally. This allows for clear data separation and ensures that cross-querying between studies is not possible.

**5.12. Data Export**

Greenlight Guru Clinical allows users to export study data (such as form answers, medication data, AE/SAE's etc.) at any time for statistical purposes – as long as users have permissions to do so. This functionality is separately protected and requires two-step verification. A user must request and verify a one-time password via SMS before being able to export data from the system. As soon as any data has been exported from Greenlight Guru Clinical, the corresponding user is responsible for complying with country-specific laws and regulations of PII. Greenlight Guru cannot be held reliable in any way, if exported data is mistreated by users which exported the data. Greenlight Guru is solely responsible for secure storage of PII data, as long as the data is kept within Greenlight Guru Clinical.

**5.13. Audit- and Transaction-logging**

All critical actions performed by users of Greenlight Guru Clinical are logged both in relation to general operations (e.g. user creation/edit) and study specific operations. study owners may review operations performed on data in relation to their own study and even export specific audit/transaction logs. Audit logging ensures that all operations performed by users can be traced. The study specific audit/transaction logs contain information about the following:

1. User which performed the operation
2. Time/date of operation
3. Affected subject/object
4. What information was changed or which operation was performed

5. Old information values (if applicable)
6. New information values (if applicable)

System specific logs are kept indefinitely and always accessible by Greenlight Guru Clinical administrative staff.
Study specific logs are kept within the specific study databases until the study owner explicit requests for study data (database) to be deleted. However, study owners can choose not to delete their study from within Greenlight Guru Clinical.

### 5.14. Deletion of Data and Study Specific Logs

Study data and its logs are kept indefinitely and securely within Greenlight Guru Clinical, as long as study owner does not explicitly request for data deletion (database deletion).

When a study owner requests for a study to be deleted, Greenlight Guru Clinical registers a “delete date” for the study - which shall be 10 days after delete request is made. After 10 days, the study specific database is deleted completely from all Greenlight Guru Clinical production services and study owner is informed of successful deletion. Any backups of the study data are kept for maximum 14 days after the database has been deleted (see why in 3.4). Afterwards, project data cannot be recovered in ANY way. Greenlight Guru has verified and validated this deletion method for every release.

### 5.15. Supported Browser

Usage of Greenlight Guru Clinical should always be performed through a supported browser. The supported browsers are:

1. Google Chrome (current version up to 2 years older versions)
2. Mozilla Firefox (current version up to 2 years older versions)
3. Microsoft Edge (current version up to 2 years older versions)
4. Safari (current version up to 2 years older versions)

Due to performance and security issues it’s recommended that users avoid the use of Internet Explorer and choose any of the other supported browsers.

It’s recommend to use the newest version of any of the above browsers, since they will contain the most up-to-date security patches.

## 6. Study Data Collection

Data collection in relation to a study conducted with Greenlight Guru Clinical is secured by only allowing users with explicit permission in a study to complete forms for a subject. Furthermore, forms that should be filled out by subjects participating in a study can only be done by following a random generated unique link sent to each subject via e-mail or SMS. E-mail/mobile verification can also be enabled on process level in relation to subject form fill out, to further validate subject identity.

## 7. Breach of Security

Greenlight Guru incorporates the latest technologies for secure computing and data storage in cooperation with Microsoft Azure. However, data transmission over the internet and data storage can never be guaranteed 100% secure. As such, if a security breach should occur, the affected customers of Greenlight Guru Clinical will be informed via personal e-mail sent to each individual user/customer. If customers do not respond to this formal notice within 3 days, contact will be taken via telephone.
A formal notice will contain the type of security breach the system was subject to and what measures have been taken to ensure minimal data breach. In addition, Greenlight Guru will inform all users of which actions to take to minimize any risk of inconvenience.
All security breach incidents are reported and documented in a standardized way, as described in Greenlight Guru internal security management procedures.

## 8. User's Responsibility

For a closer explanation of which aspects of the system are outside the responsibility area of Greenlight Guru Clinical please contact clinical.support@greenlight.guru.

### Are we Missing something?

For a closer explanation of which aspects of the system are outside the responsibility area of Greenlight Guru Clinical please contact clinical.support@greenlight.guru.

## Older versions

Version 9 From February 24, 2021
Version 8 From June 16, 2020