|  |  |
| --- | --- |
|  | **SOP Title:** Information Security Policy |
| **Study title**: *Give study title to which this SOP applies* |

# Scope and application

|  |
| --- |
| This SOP should be viewed rather as the implementation of a policy on Information Security.  This policy applies to the appropriate use of IT Systems in a way that guarantees the confidentiality, integrity and availability of clinical research data. The Information Security Policy uses the frameworks of Good Clinical Practice (GCP), ISO 27001 and the General Data Protection Regulation (GDPR). Compliance with these standards provides public assurance that the rights, safety and well-being of trial subjects are protected and that the confidentiality and integrity of data is preserved. This policy applies to all users who collect, process, store, manage, archive and dispose of data. This policy should be read together with the procedures in the Data Management Plan on how to handle and process data.  The policy applies to any information, IT systems and its related data. |

# Responsibilities

|  |  |
| --- | --- |
| **Function** | **Activities** |
| Head of IT | * Establishes and implements appropriate procedures and guidelines in support of this policy * Carries out security reviews; * Undertakes risk assessment and manage potential or actual risks at all management level; * Sets the required level of assurance, promote security awareness and record security incidents; * Security is an integral part of information systems; * The IT resources and information enable users to follow the policy as provided; * Correct and secure operation of IT facilities (physical, logical and networks among others) and resources, their integrity and availability are maintained and protected. * Has procedures in place   + to detect unauthorized information processing activities through auditing   + to control access to data and information   + to ensure that staff comply with information security policies, standard and procedures. |

# Definitions

**IT:** Information Technology

**ISO 27001:** Information security standard, published by the  [International Organization for Standardization](https://en.wikipedia.org/wiki/International_Organization_for_Standardization) (ISO).

**GCP**: Good Clinical Practice. A standard for the design, conduct, performance, monitoring, auditing, recording, analyses, and reporting of clinical trials that provides assurance that the data and reported results are credible and accurate, and that the rights, integrity, and confidentiality of trial subjects are protected.

**GDPR**: General Data Protection Regulation [2016/679](https://eur-lex.europa.eu/eli/reg/2016/679/oj) is a [regulation](https://en.wikipedia.org/wiki/Regulation_(European_Union)) in [EU law](https://en.wikipedia.org/wiki/EU_law) on [data protection](https://en.wikipedia.org/wiki/Data_protection) and privacy for all individual citizens of the [European Union](https://en.wikipedia.org/wiki/European_Union) (EU) and the [European Economic Area](https://en.wikipedia.org/wiki/European_Economic_Area) (EEA).

1. **Procedures**

# Acceptable Use Policy

Access to the IT systems is controlled by using usernames and passwords. All usernames and passwords are to be uniquely assigned to named individuals, and, consequently, individuals are accountable for all actions on the IT systems.

Users must not:

* Allow anyone else to use their accounts on any IT system
* Leave their user accounts logged in at an unattended and unlocked computer
* Use someone else’s account to access IT systems
* Leave their password unprotected (for example writing it down)
* Perform any unauthorised changes to IT systems or information
* Attempt to access data that they are not authorised to use or access
* Exceed the limits of their authorisation or specific business needs to interrogate the system or data
* Connect any non-authorised device to the network or IT systems
* Store unofficial or private data on any non-authorised device
* Give or transfer data or software to any person or organisation without the authority of the institution
* Download copyrighted material such as software and other media files without approval
* Download or install unauthorised software from the Internet without prior approval of the IT department

# Systems Access

* Access to the system will be provided and controlled by a designated Systems Administrator/Data Manager appointed by Head of IT using a formal user registration and de-registration for granting and revoking access to all information systems and services.
* The Systems Administrator/Data Manager reviews the users’ access rights at regular intervals to ensure that users are only provided with access to the services that they have been specifically authorized to use.
* The Systems Administrator/Data Manager implements appropriate access controls, and cryptographic techniques to ensure the confidentiality and integrity of data passing over public networks.
* Access to systems, networks and information should only be granted to third parties in controlled circumstances and should be approved based on the type of access and with clear reference to the reason why access is necessary. The type of access would be either physical or logical and proper controls must be applied to any such access granted.
* The Systems Administrator/Data Manager enforces complex passwords on all accounts.
* The Systems Administrator/Data Manager make sure all passwords expire after 180 days.
* The Systems Administrator/Data Manager make sure all web traffic uses secured http i.e. https://.
* The Systems Administrator/Data Manager makes sure all local accounts on the systems are provided with non-admin privileges.
* All activities on the IT systems would be logged. This provides an audit trail of system, logon, and application activities. All the logs would be periodically reviewed.
  1. **Systems Tagging and Lockdown**

All IT physical assets are recommended to be tagged electronically with warning labels and tamper proof engraved markings to always show ownership even when removed. A Database inventory of equipment showing all relevant attributes should be kept in digital form and updated when the need arises.

The IT devices deployed to the various study sites will be programmatically locked down as much as possible to allow only for purported use so that non-authorised software cannot be installed. All changes required should only be done through an authorised system change control, testing and acceptance.

* 1. **Physical Security**

All locations in which servers and other IT equipment are kept should be physically secured with access controls defining who should have access to those physical locations.

* 1. **Data and Systems Backups**

All critical data and IT systems will be protected against loss or damage in order to ensure their continued availability. Data and Systems Backups will be conducted according to SOP-WP3-19-Data Backup and Disaster Recovery. That SOP defines the systems and data to be backed up, the application used to do the backup, the frequency of backups, and the repository to keep the backup. That SOP also defines the process of restoring data and a test validation of the Disaster Recovery Plan.

* 1. **References to Other SOPs/ Policies**

This Policy focuses on Information Security and should be read together with:

* SOP-WP3-04-Data Management Plan
* SOP-WP3-19-Data Backup and Disaster Recovery.

# Attachments

|  |  |
| --- | --- |
| **Attachments** | |
| **Number** | **Title** |
|  |  |

1. **Document History and References**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | | | |
| **Version number** | **Author** | **Date** | **Description/reason for modification** |
| 1.0 | Badou Gaye  Kekuta Kandeh | 08/10/2019 | Initial version - Based on SOP\_WP3-18-Information Security Policy-v1-EN-08OCT2019  Review by Kekuta Kandeh and Badou Gaye.  Approval by Bai Lamin Dondeh and Harry van Loen. |
| 2.0 | Badou Gaye  Kekuta Kandeh | 22/06/2022 | Review to ensure that the SOP is appropriate within ALERRT and with current clinical research best practices. |

1. **Approval**

|  |  |  |
| --- | --- | --- |
| **Name and function** | **Date (dd/mm/yyyy)** | **Signature** |
| ***Author*** | | |
| *Indicate who wrote the SOP* |  |  |
| ***Review*** | | |
| *Indicate WP team members who reviewed (if applicable)* | *Date of review* |  |
| ***Approval*** | | |
| *Indicate WP Lead/Co-lead(s) who approved* | *Date of approval* |  |