GRL Information Security Policy

v1.3

Table of Contents

1. Introduction

The Information Security Policy provides guidance to individuals on how to protect the Wellcome Sanger Institute's information and Systems from malicious or accidental threats which may compromise the Confidentiality, Integrity and Availability of data.

The objective of the Information Security Policy is to preserve the Confidentiality, Integrity & Availability (CIA) of Information;

Confidentiality	Access to information shall be confined to those with appropriate authority
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification
Availability	Information shall be available and delivered to the right person, at the time when it is needed

2. Scope

This policy applies to all Genome Research Limited (GRL) employees (including Wellcome Sanger Institute, Connecting Science and Wellcome Genome Campus (WGC) operations), temporary staff, visiting workers, contractors/consultants, third parties, visitors and guests who require the use of Sanger IT systems and/or Information.

Compliance with the Information Security Policy is mandatory for all users. Should any user violate the provisions of this document or the policies and procedures in support of the Information Security Policy, either by negligence or intent, Sanger reserves the right to take appropriate disciplinary and/or legal action. In the event of non-compliance of contracted employees, this may result in termination of the contractual arrangements and/or legal action.

All users are required to adhere to the Information Security Policy in additional to policies and procedures published by the Institute e.g. the IT Acceptable Use Policy, and subsequently must acknowledge (electronically) that they have read and understood the Policy.

3. Information Security Responsibilities

Individuals who are granted permission to access Sanger's I.T Systems and/or information assets, irrespective of their status or position in the organisation is assigned the responsibility for the secure handling of all information processed by them.

Users are responsible for:

- All actions performed using their credentials (passwords, user identification etc.);
- reporting without delay, any security weaknesses or incidents to the Service Desk and/or the Head of IT Security;
- the confidentiality of Personal Identifiable Information (PII) which they may have access to;
- understanding the consequences of their actions with regard to information security practices and act accordingly, "**Security is everyone's responsibility**";
- being fully conversant with all elements of the Information Security Policy and relevant legislation, regulation, codes of conduct, policies/procedures;

4. Data access controls

All users are assigned a unique ID and unique password (for authentication) to gain access to information assets.

All information systems utilise access control measures to control access to information on a business need-to-know basis (least privileges). Access rights are immediately disabled for a user whose employment is terminated, or the rights are revoked when a user changes roles/no longer requires access.

By default Group, shared or generic accounts are strictly prohibited. For specific cases, such as 'Service Accounts', a shared account will need to be created. These accounts have a named 'owner' who is responsible for accepting and signing the 'Shared Accounts Policy'.

Account Lockout Policy: Active Directory has an account lockout policy enabled, whereby users will be locked out of their account following 10 failed authentication attempts. This policy is in place to prevent password guessing/dictionary attacks.

5. Password security

Passwords must be adequately protected;

- User Passwords must never be written down or stored electronically in clear text, divulged or shared with any individual irrespective of job role or status.

Users are accountable for all actions associated with their accounts

All user passwords (Directory Services, Applications etc.) must comply with the following:

- Initial user passwords must be unique and changed on initial receipt
- Contain a minimum 12 characters comprising a mixture of upper & lowercase letters, plus numbers. ***Ideally use a passphrase (multiple words that create a phrase), which is typically longer (and stronger) than a password.***
- Be changed when a compromise is suspected
- Not be the same as previously used passwords, or passwords used for other systems/applications

Please refer to the 'Password Policy' guidance on the intranet (Fred), for additional details.

5.1 Secrets Management

All secrets (Passwords, SSH Keys, Encryption Keys, API Tokens etc.) must be stored securely. Hardcoded passwords must be encrypted within applications and source code repositories. Access to source code repositories must be restricted to authorised individuals.

6. Sanger IT Hardware - End User Devices (Laptops/Desktops)

- Individuals are responsible for ensuring their Laptops are adequately protected from Theft or Loss e.g. not leaving devices unattended in areas where there is a risk of compromise
- All newly assigned Mac and Windows devices will have Disk encryption enabled.

- All newly assigned devices will have Endpoint Protection installed (malware detection and exploit protection)
- All Windows and Mac devices have an endpoint firewall enabled (tamper protection in place to prevent removal).
- All users must lock their screens when their device is unattended. Device screen savers are enabled following 15 minutes of inactivity for windows devices and 10 minutes of inactivity for Mac devices.
- Use of external storage devices should be avoided at all times: If there is a requirement to store Information upon external media (e.g. USB device), the IDS Service Desk will provide 'encrypted USB' devices for use. All removable storage media introduced to end user devices must be scanned for malware prior to opening.
- IDS publishes the Operating Systems (OS) supported by the Institute upon the intranet (Fred). To support OS upgrades and installation of patches, users must restart/reboot their endpoint at least weekly. Users must avoid storing unnecessary data on their device, which may prevent the OS from upgrading, due to lack of available space. If the IDS team request a restart/reboot, or upgrade, please cooperate to ensure devices are securely updated.
- Backup of end user device – If enabled by the end user, endpoint devices are backed up to backup software supported and licensed by the institute. Users are not permitted to back up their end user device to other sources.

7. Storage of Data

Sensitive data e.g. data which would cause embarrassment or reputational damage if compromised, such as Personally identifiable information (PII), must be stored upon the Internal Network Storage and/or within approved third party 'Cloud Services'. When using third party cloud services, users must consider the type of data stored and security of these services and seek approval for use from the IDS & Legal Teams.

The use of personal/non Sanger purchased Network Attached Storage (NAS) is prohibited.

In addition to specific team network directories, individuals are provided a 'personal/home directory' for personal use.

Sensitive hardcopy material (written/printed) must be safely stored to prevent loss/theft. When no longer required, this must be destroyed so that the contents cannot be read (shredded or placed within dedicated 'shred' bins for secure destruction when upon Campus).

8. Audit logging

System monitoring is in place to prevent, detect or minimise the impact of unauthorised access attempts and inappropriate IT usage, as detailed within the AUP.

9. Data Protection

Personal information (information relating to an identified or identifiable natural person) must be collected, stored and processed compliantly with all applicable data protection laws. Please see GRL's Data Protection Policy, which sets out how GRL handles and protects the personal data of its employees, temporary staff, contractors, suppliers and other third parties. All GRL staff, including temporary staff and contractors, are responsible for ensuring that GRL complies with this Data

Protection Policy, and all operational areas are charged with implementing appropriate practices, processes, controls and training to ensure that compliance.

10. Security Awareness and Training

The Head of IT Security is to provide an ongoing program of security awareness to ensure all users fully understand how information security relates to their functions.

11. Reporting of incidents

All users must report suspicious activity and IT security incidents (potential or confirmed) to it-security@sanger.ac.uk or the IDS Service Desk servicedesk@sanger.ac.uk

Examples on security incidents include;

- Hacking / unauthorised access to systems and/or data
- Unauthorised disclosure of data (business intellectual property (IP)/ sensitive data)
- Loss or theft of data/sensitive information
- Loss or theft of IT/Communications equipment
- Cracking Passwords / Keys
- Social Engineering attacks (including phishing)
- Human Error: misconfiguration of IT Systems, misdelivery of email containing sensitive data
- Misuse of information and computing resources
- Unauthorised modification of Sanger IT Systems and/or data
- Malware / Ransomware Infection
- Malicious or careless employees

12. Document Control

The Information Security Policy and associated policies and procedures are reviewed and updated at least annually, and when changes required.

Please refer to Fred for more guidance around IT and IT Security: https://fred.wellcomegenomecampus.org/Interact/Pages/Section/Default.aspx?Section=3159

Version	Author	Date	Comments
1.0	ICT	05/07/19	Version 1
1.1	ICT	19/02/2021	Updates to Storage of data, Reporting of incidents and Data Protection sections
1.2	ICT	1/4/2021	Small updates following full approval at GRL Operations Board meeting on 9-MAR-21
1.3	IDS	12/10/2022	Small updates including ICT name change to IDS, plus updates to end user device guidance.

Policy owner – Head of IT Security