POL-IGS-004 Genomics England IT Security Policy

GENOMICS ENGLAND CONFIDENTIAL UNCONTROLLED IF PRINTED

Document Key	POL-IGS-004
Title	Genomics England IT Security Policy
Document Status	Published
Confluence Document Version	v75
Published Date	May 31, 2024
Policy (only if applicable otherwise N/A)	N/A
Document Author	Ian Douglas
Document Reviewer	Grant Stapleton
Document Approver	Pete Sinden (NB To be Approved at the Data Protection and Cyber Security Steering Committee)
Details of Approval **(Completed by the QI team)**	☑ Approved in Confluence ☐ Pre-approved by email (Needs prior authorisation from the Quality Improvement Team) ☐ Reference document - approval not required
Next Review Date	☑ Default (12 months) ☐ Other - please specify
Training Format	☑ Read and understand on Confluence ☐ Course in GEL Academy ☐ Competency Assessment
Squad/Teams/Roles to be Trained	app-tr-agr,app-tr-crt,app-tr-ebt,app-tr-egh,app-tr-eop,app-tr-tgw
Template ID	TEM-QI003-003
Template Version	v18

1 Revision History

The revision history of each document is available in the Confluence Page History. To view details of what was changed, click on the versions to compare and select "Compare Versions"

2 Purpose

IT assets by their nature are likely to contain or process sensitive information. The management, tracking, control and protection of their use needs to ensure the confidentiality, integrity and availability of Genomics England assets and information. This policy aims to ensure that all Genomics England-owned IT assets, networks and access to them are managed throughout their life cycle to ensure Genomics England is meeting its legal, regulatory, contractual and licensing requirements.

3 Scope

3.1.1 In Scope

- This Policy applies to all individuals engaged by Genomics England including temporary, casual or agency staff and contractors, secondees, consultants, suppliers and data processors working for or on behalf of Genomics England. It also applies to any academic or commercial researchers with access to our research environment.
- This policy is in effect and protects all IT Assets, including laptops, mobiles, tablets, portable devices, USB devices, servers, websites, network devices and remote desktop sessions in use within Genomics England.
- The processing of all personal data, regardless of whether it is in paper or electronic format comes within the scope of this Policy.
- A failure to comply with this policy could expose Genomics England to the compromise of the confidentiality and integrity of electronic information, unavailability of information & the supporting IT assets, and/or permanent loss of data. It could also expose Genomics England to accidental or deliberate misuse of IT systems, breaches of confidentiality, corruption of data, theft of intellectual property and/or loss of availability.
- Genomics England may consider the instigation of the relevant disciplinary procedures for staff where there is evidence of deliberate non-compliance with this Policy.

3.1.2 Out of Scope

- N/A

4 Target Audience

The Genomics England controlled document is intended for an internal and (restricted) external stakeholders.

4.1.1 Internal Audience

- The internal stakeholders for the Genomics England IT Security Policy includes all Genomics England functions, teams and individual personnel.

4.1.2 External Audience

- Restricted External Stakeholders including commercial partners and academic or commercial researchers.

4.1.3 Other Third Party Audience

The external audience for this document may include medical device regulators and associated agencies in the pursuit of medical device regulatory and standards certification including:

- UK Competent Authority: (CAs) the Medicines and Healthcare Products Regulatory Agency (MHRA);
- Notified Bodies (NBs) such as BSI Group;
- NHS England (NHSE)

This document may also be requested by existing and prospective Genomics England customers as part of their procurement process. All external distribution of this document must be approved by a member of the Quality Improvements and Regulatory Affairs team prior to circulation.

5 Abbreviations/Definitions

Abbreviation	Description
Controlled Document	A controlled document is any digital or hard-copy entity which is managed within a tightly controlled process that maintains the integrity of the document's content through revisions
Data Owner /Custodian	A data owner is an individual who is accountable for a data asset. This is typically an executive role that goes to the department, team or business unit that owns a data asset.
Document Control	Those tools, systems and procedures put in place to ensure project critical documents are kept up-to-date, available and fitforpurpose. The result of good document control ensures staff have access to the current document for the activity they are performing.
Personal data	Personal data means ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’ This may include an individual’s: · Name (including initials); · Address; · Identification number; · Location data; · Online identifier, such as a username or IP address. · It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity. **Personal data is only information concerning a living person.**
Personal data breach	Personal data breach means breach, or suspected breach, of security leading to or which may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Special categories of personal data	Personal data which is more sensitive and so needs more protection when processed. The categories are defined in Article 9 of the GDPR: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

6 Introduction/Background

This Policy incorporates:

- The requirements of Data Protection Act 2018 and the UK General Data Protection Regulation 2018. This document is also based on guidance published by the Information Commissioner's Office (ICO)
- Advice and guidance from the National Cyber Security Centre
- Advice and guidance from NHS Digital on Information Security and Data Breaches.
- Aspects of the ISO 15189 requirements including the identification and control of non-conformities (4.9), corrective action (4.10), preventive action (4.11) and continual improvement (4.12).

Genomics England shall comply with the following legislation and other laws as appropriate:

- The Data Protection Act 2018
- The UK General Data Protection Regulation
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The common law duty of confidence
- Regulation of Investigatory Powers Act 2000 (RIPA)
- The Freedom of Information Act 2000
- Health & Social Care Act 2015

7 Authorities and Responsibilities

Role	Responsibilities
All staff, secondees, researchers and suppliers	To be aware of information governance compliance. To read and understand this Policy. To report all data security and protection incidents and personal data breaches to the Genomics England Service Desk without delay.
Caldicott Guardian	The Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
Data Protection Officer (DPO)	The DPO will provide advice and guidance on data security and protection incidents involving personal data. The DPO will act as the contact point for the ICO, and any other external regulatory body.
Chief Medical Officer	Acts as the key interface with NHS England and leads the Genomics England Clinical Teams.
Executive Director	The Executive Director is the board member with overall responsibility for Information Governance and Data Protection.
Head of Information Security	Responsible for maintaining this policy and ensuring it is up to date, reflects the Genomics England position on this subject and remains relevant to the threats and risks posed to Genomics England. To manage all Information Security incidents To work collaboratively with all stakeholders in delivering effective Information Security best practice.
Head of Service Management	The Head of Service Management has overall responsibility for the Service Desk.
Senior Data Protection Manager	To manage all data protection incidents, including personal data breaches from reporting to closure. To work collaboratively with all stakeholders in delivering effective Information Governance best practice.
Platforms & End User Tech teams	Mandate and provide the appropriate centralised IT asset management stores for the receipt of Genomics England IT Asset Device information, as required by Genomics England Policies and/or legal, regulatory, contractual or licensing requirements. Ensure appropriate levels of access are granted to IT assets under their control in alignment with this policy. Ensure a clear inventory of assets is maintained and communicated as part of Genomics England BAU activities.
Senior Information Risk Officer (SIRO)	The SIRO has overall responsibility for ensuring that effective systems and processes are in place to address the Data Protection agenda. The SIRO is responsible for information risk within the organisation and the provision of written advice to the Executive Leadership Team on the content of the Governance Statement in regard to information risk.
Service Owners	Accountable for the secure running of their services
Product Owners	In conjunction with Service Owners are Responsible for the secure running of their products

8 Procedure Details

8.1 Staff responsibilities for Information Security

All Staff are required to sign a confidentiality code of practice upon commencing employment with Genomics England (whether that is on a full time, part time, secondment or temporary basis). Contracts with external contractors that allow access to Genomics England's information systems must be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of external organisations comply with all appropriate security policies.

All Staff are required to comply with information security procedures. Staff will comply with Information Security awareness training which will be included in the staff induction process and be responsible for the operational security of the information systems they use. An ongoing awareness programme will be established and maintained to ensure that staff awareness is refreshed and kept up to date.

Researchers are bound to comply with the terms of their access and must undergo data protection and cyber security training as directed by Genomics England.

8.2 Account Management & Authentication

8.2.1 Access Control

- All user accounts must be linked and readily identifiable as belonging to an individual.
- All accounts created must have an associated, and documented, request and approval.
- Genomics England centrally managed accounts (i.e. Azure, Okta etc.) should be used. The use of local user accounts should be avoided and must be documented as part of an approved design.
- Service Owners or their authorised delegates are responsible for the approval of all access requests.
- User accounts and access rights for all Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
    - Accounts or privileges no longer needed must be removed promptly after a review is completed.
    - All Genomics England accounts must be reviewed on a periodic basis, for activity, privilege and security.
    - Staff accounts will be disabled after 30 days inactivity
    - Supplier Contractor accounts will be disabled after 15 days inactivity
    - External user accounts, such as GECiP and industry partners, will be disabled after no more than 90 days inactivity
- Under no circumstance must individuals share passwords or authentication tokens.
- All Genomics England systems must enforce the use of individual accounts and authenticate these accounts in accordance with this policy.
- Confidential data access must be logged.
- User Identity will be continuous verified and validated, and the user session should be no longer than 12 hours.
- Particular care must be taken in any process around the issuing or re-activation of a user account. The process must have robust steps to ensure the requestor is authorized and authenticated. This is to prevent social engineering attacks against teams such as the service desk etc.

8.2.2 Authentication

- All services should use GEL standard identity provider.
- Passwords with the following characteristics can be used for all systems.
    - Passwords should never be based on *single* dictionary words, User Ids, personal information (Car Registration, Spouse, Children's or Pet's names, birth dates etc) and special care should be taken to avoid common industry terms or easily guessable combinations of words.
    - Passwords must be hard to guess by another person while easy to remember by the owner.
    - Passwords must be at least 12 characters long.
    - As per the advice of the National Cyber Security Centre (NCSC Guidance on password expiration https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry.) regular changes in passwords are not required, however, passwords should be changed if there is any indication that they may have been compromised.
- Mobile Devices must be protected with a passcode of a minimum of 6 characters.
- Multi-factor authentication shall be considered the 'standard' for Genomics England and must be implemented across all systems. It is especially important that accounts with privileged access (e.g. "root", "admin" etc.) shall be multi-factor authenticated
- All Genomics England systems must enforce an account lockout upon the receipt of 5 incorrect/failed password login attempts.
- IT Systems must implement a password protected screensaver or other mechanism, with a timeout setting of 2 minutes or less, to protect from unauthorised access when left unattended.
- All Genomics England processes and systems must incorporate appropriate separation of duties, based on the business risk of the data being processed.
- All Genomics England processes and systems must employ the concept of least privilege, allowing only authorised actions or privilege for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with documented requirements.
- All access to Genomics England systems with either individuals accounts or elevated privilege accounts (such as admin or root) must be logged in accordance with requirements of this Information Security Policy.
- Passwords or other secrets (e.g. DB credentials , API connection strings, etc) must not be stored in plain text in scripts, code, documents or any other location without suitable access controls and security protection. The use of Password Vaults or Secrets Management systems must be used in preference to other solutions.

8.2.3 Privileged User Management

- Privileged access using "root" or "admin" accounts must be documented or controlled in a way that ensures actions taken by that account can be traced back to an individual.
- All access to Genomics England systems with either individuals accounts or elevated privilege accounts (such as admin or root) must be logged in accordance with requirements of this Information Security Policy.

- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Personnel with Administrative/Special access accounts must have regularly Access Review that is documented.

8.2.4 Service Account

Service accounts are special accounts used by systems/components to authenticate to other systems/components without user interaction.

- Service Accounts must have an owner accountable for mitigating security risks.
- An updated inventory of all service accounts should be maintained.
- The concept of least privilege must be followed when creating service account, and the scope of the service account should be limited.
- Service accounts that accessing sensitive and critical data must be documented and approved by the appropriate Design Authority (including representation from the Security Team)
- Service accounts credentials should be stored in appropriate Secret Management Tool such as AWS Secret manager.
- All service accounts must have auditing enabled.

8.2.5 Supplier Access

- Supplier access must comply with all existing policies.
- External Supplier access activity must be monitored.

8.3 Secure Use of Cloud Services

All cloud-based services must be approved prior to acquisition and deployment. To ensure secure adoption and usage of cloud services, the following steps must be taken:

- Define organisational needs and priorities.
- Define service users, both internal and external.
- Determine the type of cloud service to be adopted, including the physical and operational characteristics for SaaS, PaaS and IaaS solutions.
- Define the data types to be stored.
- Determine the security solutions and configurations required for encryption, monitoring, backups, etc.
- Generate a list of past security incidents involving this cloud provider.
- Request available security certifications.
- Obtain copies of agreements with the provider, including SLAs.

8.3.1 Inventory

- An Inventory of cloud services in use must be maintained and reviewed at least quarterly

8.3.2 Approved Cloud Services

AWS (and other external provided) services must be approved before they either store 'live' data of any classification or be connected to other services handling live data. New services must be approved via appropriate governance bodies such as a Design Authorities and where necessary have received approval from Information Governance and/or Cyber Security teams.

8.3.3 Cloud Service Risk Assessment

Where required Cyber Security team shall conduct a risk assessment at the following times:

- Upon the implementation of a new cloud service

The cloud security risk assessment shall include the following:

- Audit results, both internal and external (cloud provider system security audit results)
- Threat and vulnerability analysis
- Regulatory compliance

8.3.4 Unauthorized Services

Any service that is not explicitly approved is by default an unauthorized service and must not be used to store or process Genomics England data of any classification.

8.3.5 Cloud Security Controls

Tools for centralised visibility of the cloud service infrastructure, such as cloud workload protection (CWP) tools must be implemented. The tools shall offer traffic analysis, configuration monitoring and assessment, and alerts for configuration issues.

The Cloud Security Administrator shall perform an assessment of security control configurations and all failed attempts of unauthorised access monthly.

8.4 IT System and Device Security

8.4.1 Email Use

- Users must only use email in accordance with acceptable use policies and/or requirements laid out in the the employee handbook
- Users must not set up any ‘auto-forward’ rule to automatically forward emails to external email addresses

8.4.2 Encryption

- Data must be encrypted at rest (i.e. when stored). Best practice dictates non-sensitive data should be encrypted at rest. The Head of Information Security must approve alternate controls when encryption is not possible or other mitigating controls are in place.
- Removable media (USB Drives etc.), laptops, mobile phones, tablet, etc. must always be encrypted.
- Data must be encrypted in transit (i.e. network communications) on external networks.
- Data must be encrypted in transit (i.e. network communication) on internal Genomics England Networks unless the lack of encryption is specifically detailed in an architecture design that has been approved by the Head of Information Security
- Encryption algorithms used must meet current industry best practice (for example AES 256, etc.)
- Encryption keys must be managed to ensure that data is protected
    - Encryption keys must be remain with the control of Genomics England. Specifically in AWS this means the use of Customer Managed Keys
    - Keys must be regularly rotated and the duration and process for changing for each key must be documented by either the infrastructure of application owner
    - Keys must be **immediately** rotated if there is suspicion they may have been compromised
    - Access or alteration of keys must be logged and auditable

8.4.3 Configuration Management

- All IT Systems must be built from a standard configuration for that Operating System and purpose.
- All standard configurations shall be hardened according to an appropriate documented configuration standard, and systems built from these standards then hardened further where appropriate.
    - As part of this hardening, all unnecessary system utilities and services must be removed.
    - Additionally, all administrator access or privileged accounts must be removed or restricted.
    - Default passwords must be changed
- Industry best practice guides (as published by organizations such as CIS, NIST, NCSC) or vendor best practice guides (such as the AWS Well Architected Framework) should be used to guide configuration standards
- Genomics England must also comply with standards and guides published by the NHS where applicable (e.g. the NHS-England guide on public cloud usage).
- All above used configuration standards shall be documented and approved by Genomics England Head of Information Security.
- AWS Security Hub assesses the Genomics England AWS Estate against both CIS and NIST 800-53 standards. Service Owners and accountable for ensuring findings are regularly monitored and remediated against
    - In line with vulnerabilities Critical and High rated findings must be remediated in 14 days of the finding.
    - Medium and lower rated findings should be remediated within 90 days

8.4.4 Patch Management

- Service owners are accountable for ensuring that Vendor releases of patches and fixes for IT systems are monitored for on a regular basis and patches applied with due consideration of the criticality and exposure of the system and patched vulnerability.
- System owners are responsible for monitoring the systems they are responsible for to ensure adequate time can be allocated to patching.
- All software must be licensed and supported.
- Patches must be deployed according to the severity of the vulnerability, risk and the criticality of the system.
- Patching for vulnerabilities classed as 'Critical' or 'High' must be completed within 14 days of vendor issuing a patch.
    - Vulnerabilities are counted for all resources in all AWS accounts whether they are in active use or not.
    - NB: Critical and High is based on the AWS Inspector tool that Genomics England uses to identify vulnerabilities and is defined as a score above 7.0 on the CVSS Score (Common Vulnerability Scoring System). This is in order to be compliant with the UK Gov Cyber Essentials certification standard.
- Vulnerabilities scoring between 4.0 and 6.9 (Medium) on the CVSS scale should be patched regularly and no later than 90 days after publication.
- The patching process must be documented, regular and repeatable.
- All users, including remote and home workers, are required to, at least once a month, ensure that system upgrades, anti-virus definition upgrades and information security patches are applied to their laptops, mobile phones. Tablets etc.
    - Users must accept and apply patches and updates when available
    - Users are responsible for keeping software that they have installed patched in line with the policy requirements detailed above

8.4.4.1 Exception Process

A formal exception process\committee owned and chaired by the SIRO (Senior Information Risk Owner) will consider exceptions. For an exception to be granted the following must **ALL** be true

- The risk has been assessed and is deemed acceptable. This will take into account other risk mitigating factors, the ease of exploit, the current threat landscape etc.
- There must be a credible plan to fix the vulnerability by an agreed date (typically in the next sprint, maintenance window or release)

8.4.5 Malware Protection and Prevention

- Malware detection and anti-malware and repair software being of good industry standard and approved by Genomics England security must be installed on all information systems connecting to Genomics England’s networks.
- This software must be active, be set to a configuration approved by the Head of Information Security and kept up to date.
- All files, including e-mail attachments, originating from external sources (e.g. the Internet, external party networks and removable media) must be scanned as close to the point of entry to the Genomics England’s network or assets as possible and in real time.

8.4.6 File Integrity Monitoring

- For systems deemed high risk (i.e. failure could cause a severity 1 or severity 2 level incident), critical configuration and/or data files should be monitored for unauthorised change or access, and this detection then logged and monitored as per the section covering Security Logging and Monitoring later in this policy.

8.5 **Network Security**

- All new major network changes, connections and access to Genomics England networks shall only be granted following a Risk Assessment conducted by the Information Security Team and requesting.
    - The security controls may include access restrictions, physical and/or logical segregation, and secure traffic filtering.
- All connections to un-trusted networks, such as the Internet, must be protected by an approved firewall or other approved security device, with no direct access allowed between trusted and un-trusted networks, nor shall any access between these networks be allowed to bypass the authorised gateways, proxies or controls.
- Firewalls or other network segregation services/devices must be chosen to appropriately manage the risk posed to the trusted network and the assets it holds, including infrastructure and applications at all layers of the network “stack. These devices or applications must be approved by Genomics England Security before use.
    - All firewalls should be implemented with the intent to transmit “good” traffic and stop or otherwise prevent “bad” or unauthorised traffic from being transmitted, independent of what layer or level this traffic conforms to.
    - All firewalls must enforce traffic control on a “default deny” basis.
    - All firewall or other service configurations must be configured to ensure that all traffic from and to trusted networks shall be restricted to specific named hosts, networks and specific applications on these hosts, or other appropriately controlled access, as approved by the Information Security Team.
- All network security devices (firewalls, routers, switches) must be configured according to documented standards approved by the Information Security Team.
- All network security device configurations shall be reviewed on an annual basis to verify configurations and the security benefit provided.

8.5.1 Remote Access

- Remote access to Genomics England networks or Information Systems shall be provided using one or more remote access servers employing transport or IP level encryption. The configuration of such servers shall be documented by the system owner and approved by the Information Security Team.
- Network level connections (for example a VPN connection) or other privileged access (such as AWS Console must only be made to or from locations in the UK or GDPR compliant countries. Technical mechanisms such as Geoblocking on firewalls may be used to enforce this control.
- All remote access connections to the networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
- Remote users may connect to the networks only after formal approval by the requestor’s manager.
- Remote access to Information Resources must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the network unless approved in advance by Cyber Security Team.

8.5.2 Network Architecture

- All networks used for Genomics England traffic shall be managed and designed in accordance with approved architectural designs and configurations, with appropriate layered security controls and network segmentation.
- All networks must be documented appropriately, with this documentation kept updated and reviewed periodically.
- Network documentation shall include:
    - Network configuration diagrams, showing nodes and connections;
    - An inventory of communication equipment, software, links and services provided by External Parties;

8.6 **System Development, Acquisition and Release**

8.6.1 Security Requirements of IT Systems:

- Information security requirements (functional and non-functional) must be considered in the acquisition or development of new IT systems or enhancements to existing ones.
- The procurement process must include sign off from the Cyber Security Team where necessary
    - Security requirements must be included in the decision to purchase and deploy Commercial Off the Shelf (COTS) software, Open Source software and cloud based services.
    - Identification and management of information security requirements and associated processes should be integrated in the early stages of acquisition or development of IT systems projects, and then incorporated through the entire lifecycle of the project and the solution.
    - Information security requirements and controls should reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security.
- Security requirements shall be provided by the security team and be based on risk assessment of the data to be processed by the system.
- Where systems are operated or accessed over untrusted networks, ensure they are developed to protect communication.

8.6.2 Secure Systems Development

All developed software and systems (either developed by Genomics England staff or on behalf of Genomics England by third party suppliers) shall follow a secure lifecycle approach, which includes:

- Business strategy, plans and roadmaps for software development, acquisitions operation and decommissioning.
- Secure engineering principles, including modelling, testing, reliability and resilience shall be used.

- System and security requirements are included and documented. Designs must be approved by the required governance body (i.e. a Design Authority)
- Development has demonstrable testing and acceptance criteria.
- All testing and acceptance criteria are documented and provided to Genomics England as part of the acceptance criteria.
- Systems are tested to ensure the system and security requirements are met.

8.6.3 Security in Development and Release-into-Production Processes

- Ensure that Development, Testing and Production environments are available and logically or physically separated with change control and appropriate security testing in place before promotion of releases or code between these environments.
- Evidence of security testing must form change approval process i.e. be included in the CAB (Change Approval Board) ticket

The system owner or product manager is responsible for ensuring that the following controls are in place:

System security testing

- System security testing must be executed regularly during development cycles.
- System acceptance testing must be developed for new systems, upgrades, and system versions.
- Test and acceptance criteria must be developed based on the functional, non-functional and security requirements.
- Testing must include OWASP for applications as well as bespoke testing based on assessed threat modelling.

Use of Test Data:

- The use of operational data or data containing personally data or any other confidential information for testing purposes must be avoided. If personally data or otherwise confidential information is used for testing purposes, all identifiers, should be removed or pseudo anonymised. Unless the data is anonymised beyond recognition of individuals. Refer to the guidelines on anonymisation provided by the ICO.
- All test data must be removed from systems before promotion to production and retained securely to prevent contamination.

System Acceptance

- System acceptance criteria must be developed, which includes, assessments against the functional and non-functional requirements.
- Testing and remediation for internal and externally developed systems shall be provided, which must include remediation of any residual security vulnerabilities.
- All back-doors, covert channels and hooks must have been removed before the application is approved for operation.
- A minimum set of security and operations documentation, procedures and maintenance documents, that include update schedules, roadmaps, operating instructions and all software modules utilised and any licensing agreements.

8.7 **Security Logging and Monitoring**

- All security devices and/or software resident on IT systems must log security data where possible.
- IT systems must log critical activities, activities of critical accounts or access to critical data or programs, or any combination thereof.
- Log entries should capture at a minimum the following information:
- Date, time and time zone;
- Information, event, alert, failure, software and/or configuration changed, data accessed
- Location of change (hostname, filename or table name).
- Additionally, where possible, the following information should be captured:
    - User (individual user\ proxy user, account name, etc) associated with an event
    - Originating IP Address
    - Original value where possible;
    - New value (other than for changes such as a password change); and what has been changed.
    - Relevant description of message of the event
- Suspicious or unauthorized activities must be identified and prioritized based on an understanding of the threats faced by the systems and the way in which these may occur.
- An alerting process with prioritisation of events must be developed. This process must be reviewed and evaluated on a regular basis.
- Where possible, alerts must be sent to designated personnel for high-risk suspicious activities for immediate review and response.
- All logs must be reviewed regularly for the identified suspicious or unauthorized activities and appropriate action must be taken.
- The frequency of the review will depend on the threats /risks involved. Risk factors that should be considered include:
- The criticality of the application processes;
- The value, sensitivity or criticality of the information involved;
- Prior incidents of system infiltration and misuse;
- The extent of system interconnection.
- Audit trail of review and actions taken must be maintained.
- Where possible, automated methods of log aggregation across different systems, event correlation and pattern detection should be used. It is recommended that either a centralized log repository collects information from participating systems using non-privileged read-only accounts, or the participating systems push log information to the centralized log repository.

8.7.1 Retention

- Logs with security relevant information (as discussed above) must be maintained for a minimum of 1 year, or such longer period as is defined in the relevant logging standard for that system, or for such longer period as is required for legal, regulatory or contractual compliance.
- Logs may be kept online or offline, in a secure fashion, but must be recoverable within a reasonable period.

8.7.2 Log Security

- Logs must be considered to contain sensitive information and protected accordingly.
- At a minimum the following principles must be followed:

- Mechanisms must be put in place to ensure logging cannot be deactivated and logs cannot be modified or deleted in an unauthorized manner. Where possible, logs should be automatically monitored for sudden decreases in size and gaps in log entry sequence.
- Access to logs must be provided on the basis of need to know and least privilege.
- Where possible, log files should be protected by cryptographic hash.

8.8 **Vulnerability Detection and Management**

- Please refer to POL-IGS-006 Vulnerability and Technical Assurance Policy

8.9 **Ransomware Policy**

- In line with UK Government policies and guidelines, Genomics England will **not** pay ransoms in the event of a ransomware attack.

8.10 **Training and awareness**

Genomics England staff and all those accessing Genomics England data, such as researchers, are required to undertake data protection training as part of their induction process and this must be repeated annually. Staff including the Executive Team, Caldicott Guardian, SIRO, Data Protection Managers and the DPO may undertake additional specialist training.

8.11 **Monitoring arrangements**

The Senior Information Risk Owner is responsible for monitoring compliance with this Policy.

Genomics England adheres to a number of external Standards to ensure a minimum standard for the completion of processes, for example IS0: 15189. The ISO 15189 standard supports the Quality Management Framework within Genomics England that includes monitoring compliance with SOP's and Policies.

9 Supporting or Reference Documents

SOP-IGS-002 Data Security and Protection Incident

POL-IGS-001 Data Protection Policy

10 Appendices

N/A