ALLOCATE

Cloud Services

Technical and Organisational Measures

Data in transit protection

Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.

All Allocate Cloud network traffic is also encrypted via SSL using high strength 2048Bit encryption, only SSL is allowed in all instances providing a secure delivery approach.

Any data migrated in or out of the Cloud environment is encrypted with a strong password and transmitted via a secure FTP.

Asset protection and resilience

Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

All Cloud environments are within Tier III+ Datacentres with virtualised resilient infrastructure, network topology with multiple points of presence.

- 24/7/365 manned security
- 24/7/365 CCTV onsite and monitoring
- Front desk reception checks
- Numerous ID card gateways
- Man-trap entry systems
- 24/7/365 support offered by in-house qualified engineers
- ISO 27001 / ISO 9001 and PCI compliance
- Full inert gas fire suppression system
- Network-monitored, highly sensitive VESDA fire detection system

Data at rest protection

Backups are encrypted at system level using 256 Bit AES encryption. Only a minimum of senior authorised staff at Allocate Software have access to the authentication password for restoration.
Backups are taken for a full bare metal restore state and also a copy of system drives for data.

All access is carefully controlled to ensure that only the relevant people have access for critical administration tasks. All staff also sign a non-disclosure agreement for confidentiality.

Ordinarily we collect, process and store personal data in the UK or within the EEA (usually as part of our operations in Ireland). However, we reserve the right to do so

(i) anywhere within the EEA (and, if legally permitted, to continue to do so following any withdrawal of the UK from the EU) and

(ii) where personal data has been collected in any of the other countries in which we operate

Similarly, we reserve the right to collect, process and store personal data

(i) in any country which has been assessed by the appropriate regulatory authority as providing necessary protection for the rights of data subjects in connection with the processing of their personal data, or

(ii) in other countries where we have taken steps to ensure that the transfer of personal data is in line with the UK data protection requirements and will be protected and treated securely. Note that organisations outside of the EEA may be required to provide personal data to foreign authorities.

Data sanitisation & Disposal

Data will be retained for 7 years or the life of the contract. When no longer required or usable, tape cartridges, hard copies, and other similar items used to process or store classified and/or sensitive data shall be properly disposed of.

The following procedures will be followed:

- Diskettes, tape cartridges or hard drives shall be handed to the Allocate Group Information Services team for secure destruction via a certified 3rd party provider.
- Computer electronic files containing sensitive date are deleted and removed from any common shared locations or personal storage devices when they are no longer justifiably required for retention.
- Redundant Databases and data file areas will be deleted so to be reasonably recoverable whilst retaining the integrity of the host storage area i.e. SAN Array.
- Any data sanitization activities are vetted and signed off by a senior manager.
- Disposal of computer equipment is to be carried out by a reputable specialist disposal firm and disposal records are kept for both Information Security and Environmental reasons.
- Any redundant and potentially sensitive files will be data sanitised. Being completely removed ensures that information cannot be recovered using file recovery tools.

Physical resilience and availability

- Geographically separate Datacentres
- 99.8% uptime SLA excluding planned downtime
- Highly scalable infrastructure to meet future growth demands
- Disaster Recovery (This allows us to bring the service up from an alternative datacentre in a different location in the event of a disaster such as fire, flood or major disruption to power or telecoms).
- 8hr Recovery Time Objective / RTO – this is the time it will take us to recover the system to new a new geographic location should a major disaster occur at the primary site such as a fire or flood.
- 24hr Recover Restore Objective/ RRO – we use the previous night's backup to recover from a disaster, so the maximum amount of time and work lost would be 24 hours. Higher levels of service are available as options.
- High Availability secure Internet connection

Separation between consumers

Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.

- Data is segregated by unique database credentials per customer.
- Databases are unique per customer.
- Databases are encrypted.
- Internal IPv4 database traffic is secured to unique ports per customer.

- Application instances are isolated on standalone implementations unique to each customer.
- IaaS model shares hardware such as networks, storage and compute power.
- Aggregated data used for benchmarking, logging and comparisons may be stored in segregated databases and reported anonymously.

Independent testing of implementation

Independent penetration testing is carried out for each release with a CHECK, CREST and TIGERSCHEME accredited tester. Providing assurance of secure controls, each service is tested quarterly with regular infrastructure tests.

Governance framework

The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.

Allocate operate clear governance practices. Our governance framework is ISO27001 certified and independently validated:

Certificate No. 143704-2013-AIS-GBR-UKAS

Allocate Software Limited are registered with the Information Commissioners Office:

Registration Number: Z7285503
Date Registered: 28 October 2002 Registration Expires: 27 October 2019
Data Controller: Allocate Software Limited

IG toolkit
Allocate Software 8HC03
Allocate Software PLC (London) 8HJ28

Cyber Essentials - IASME-A-03954

Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- goods and services
- employment and education details
- financial details
- information necessary for the development and test of software

Allocate Software are registered as a commercial third party with NHS Digital using the version 14 information governance toolkit under organisation codes 8HC03 & 8HJ28.

Operational security

The service provider should have processes and procedures in place to ensure the operational security of the service. Allocate operate the following operational processes:

- Configuration and change management - ensuring that changes to the system do not unexpectedly alter security properties and have been properly tested and authorised.
- Vulnerability management - ensuring that security issues in constituent components are identified and mitigated.
- Protective monitoring – taking measures to detect attacks and unauthorised activity on the service.
- Incident Management - ensuring that service can respond to incidents and recover a secure available service.

Configuration and change management

Allocate Cloud operates to an ITIL aligned configuration and change management process.

- The status, location and configuration of service components (including hardware and software components) are tracked throughout their lifetime within the service.
- Changes to the service are assessed for potential security impact. Changes are managed and tracked through to completion.

Allocate Cloud operates a well-defined incident management process.

Vulnerability management

Allocate closely monitor for known vulnerabilities and act accordingly to mitigate:

- 'Critical' patches deployed within 14 calendar days of a patch becoming available
- 'Important' patches deployed within 30 calendar days of a patch becoming available
- 'Other' patches deployed within 90 calendar days of a patch becoming available

'Critical', 'Important' and 'Other' are aligned to the following common vulnerability scoring systems:

National Vulnerability Database Vulnerability Severity ratings: 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST)

Microsoft's Security Bulletin Severity Rating System ratings: 'Critical', 'Important' and the two remaining levels ('Moderate' and 'Low') respectively.

Protective monitoring

Allocate collect multiple types of audit information and it is regularly analysed. Basic intrusion detection technologies are in place at the perimeter devices. Applications and services are monitored and reported in real time to the Allocate Operations monitoring center.

Incident management

- Security Incident processes are in place for the Allocate Cloud service and are enacted in response to security incidents.
- Pre-defined processes are in place for responding to common types of incident and attack.
- A defined process and contact route exists for reporting of security incidents by consumers and external entities.
- Security incidents of relevance to them will be reported to customers in acceptable timescales.

Personnel security

Service provider staff should be subject to personnel security screening and security education for their role.

All privileged access is carefully controlled to ensure that only the relevant people have access for critical administration tasks. All staff are required to sign a non-disclosure agreement for confidentiality.

Allocate operate robust pre-employment screening, effective line management, employee welfare, clear lines of communication, and a strong security culture. This also includes a formal process for managing staff leaving the business. Regular security training is given appropriate to role.

Secure development

Services should be designed and developed to identify and mitigate threats to their security.

- New and evolving threats are reviewed, tested and the service improved in line with them.
- Agile Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.
- Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

Allocate carry out quarterly service reviews of our infrastructure supply chain and ensure service levels are maintained alongside ISO accreditations and IG compliance.

Secure consumer management

Consumers should be provided with the tools required to help them securely manage their service.

Allocate Cloud customers are authenticated using a predefined approved users list before being able to perform management activities, report faults or request changes to the service.

These activities may be conducted through the Allocate Customer Support web portal, or through other support channels (such as telephone +44 0844 417 9510).

Identity and authentication

Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.

- Allocate cloud supports federated authentication services for single sign on
- Access to core applications can be configured using a dedicated encrypted tunnel
- Strong and complex passwords are required
- The system provides an integrated, flexible and comprehensive set of security facilities in order to allow only authorised access to those parts of the system appropriate to a particular type of users

External interface protection

All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.

All external Allocate Cloud interfaces are tested.

Independent penetration testing is carried out for each release with a CHECK, CREST and TIGERSCHEME accredited tester. Providing assurance of secure controls, each service is tested quarterly with regular infrastructure tests.

Secure service administration

The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.

The Allocate Cloud uses dedicated devices on a segregated network. Dedicated devices for service management purposes are used to manage the service from a segregated management network.

The devices are used solely for service management, and not for general purpose use, such as email and web browsing.

Using this approach, the management devices and segregated network are difficult to attack.

Audit information provision to consumers

Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.

Audit functionality allows users to:

- Store of rosters as required for clinical governance issues
- Provide secure access to the system with different user access levels to see / update data as required (e.g. only certain users can add overtime).
- Provide full audit logging of what user made what changes with both time and date stamps
- Allow rosters to be 'locked down' after they are finalised to prevent unauthorised changes.

In addition, integration of our solution to Microsoft ADFS provides logging of user connections.

Audit trail of changes to data, all data changes made to a HealthRoster Database, be they Inserts, Updates or Deletes are logged to the internal Activity Log Tables (ACTIVITY_LOG and ACT_ITEM_CHANGE_LOG). The ACTIVITY_LOG records the Table level change and the ACT_ITEM_CHANGE_LOG records the details of the changes. These can be reviewed or displayed to users as appropriate (they are not normally displayed to users by default).

Secure use of the service by the consumer

Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

The Customer shall comply with the following responsibilities:

(i) The Customer shall inform Allocate of any change of use, or intended change of use of the Operational Service. For example, if the server is to be made available to a different user base, or a significant change of content is to be planned, or the Customer exceeds the agreed pricing parameters (number of Rostered Units and Number of Employees) then Allocate shall be informed;

(ii) If such a change results in a change to the charges, Allocate will advise the Customer of this prior to its implementation. In any case Allocate may still need to change its infrastructure allocation.

(iii) The Customer is responsible for all data security issues, excluding those pertaining to the control of access by Allocates own staff. This includes ensuring usernames and passwords are managed in a secure way and ensuring data is not made publicly available where inappropriate.

(iv) The Customer shall inform Allocate in advance of any changes to its infrastructure (network, firewalls and other equipment) that might have an impact on the Allocate Cloud Infrastructure.

Security Incident Policy

Allocate Software plc. is responsible for the security and integrity of all data it holds. Allocate Software plc. must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to our or customers assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security:

A computer security incident is an event affecting adversely the processing of computer usage. This includes:

- loss of confidentiality of information
- compromise of integrity of information
- denial of service
- unauthorized access to systems
- misuse of systems or information
- theft and damage to systems
- virus attacks
- intrusion by humans
- Other incidents include:
- Loss of ID badge/s
- Missing correspondence
- Exposure of Uncollected print-outs
- Misplaced or missing media
- Inadvertently relaying passwords

Responsibilities

Management of security incidents described in this policy requires Allocate Software plc. to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide Guidance

Network Access

The Allocate Software plc. has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing Allocate Software

plc. employees, elected members, partner agencies, contractors and vendors of the importance of the identification, reporting and action required to address incidents, the Allocate Software plc. can continue to be pro-active in addressing these incidents as and when they occur.

All Allocate Software plc. employees, elected members, partner agencies, contractors and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via the Allocate Software plc.'s Incident Reporting procedures.

The types of Incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended

Users of Allocate Software plc. computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Allocate Software plc. Employees, elected members, partner agencies, contractors and vendors need to ensure they lock their computers appropriately - this must be done despite the fact that Allocate Software plc. computers are configured to automatically lock after 15 minutes of idle time.

Discovery of an unlocked computer which is unattended must be reported via the Allocate Software plc.'s Incident Reporting procedures.

Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the Transformation Service must be notified through the Allocate Software plc.'s Incident Reporting procedures. For more information, the Allocate Software plc. Password policy is available on the intranet (Dnet) or via the Transformation Service's Service Desk. Under no circumstances should an employee allow another employee to use their user account details after they have logged onto a system – even under supervision.

Virus warnings/alerts

All Desktop, laptop and tablet computers in use across the Allocate Software plc. have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Allocate Software plc. data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to Group Information Services as soon as possible.

Media loss

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental

of any portable media must report it immediately through the Allocate Software plc.'s Incident Reporting procedures.

Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised -recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Allocate Software plc.'s website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All Allocate Software plc. Employees, elected members, partner agencies, contractors and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Allocate Software plc. data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using the Allocate Software plc.'s Incident Reporting procedures

Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc… must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person identifiable information must be reported through the Allocate Software plc.'s Incident Reporting procedures.

Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the Transformation Service via the Allocate Software plc.'s Incident Reporting procedures.

Continuing emphasis and re-enforcement of the Allocate Software plc.'s Secure Desk policy will further help to reduce the number of security incidents.

Logical Security / Access Controls

Controlling, managing and restricting access to the Authority's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

Missing correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc… must be reported through the Allocate Software plc.'s Incident Reporting procedures.

Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through the Allocate Software plc.'s Incident Reporting procedures.

Loss or theft of IT/information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc… or which is known/or suspected to have been stolen needs to be reported immediately through the Allocate Software plc.'s Incident Reporting procedures

Incident Reporting

Reporting via GIS

Security incidents and breaches can be reported by telephoning the Group Information Services Team on:

+442030436944

Reporting via Email

Low risk security breaches may be reported via e-mail to the Group Information Systems Team however, wherever possible, confidential or personal identifiable information should not be contained in the e-mail e.g. logon passwords.

isupport@allocatesoftware.com.

Incident Management

When an incident is reported and entered into the call logging system, an email is generated and sent to the Information Security Manager. The Information Security Manager will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representative to deal with as soon as possible. Representatives looking into security breaches will be responsible for updating, amending and modifying the status of incidents in Service Manager.

All parties dealing with security incidents shall undertake to:

- analyse and establish the cause of the incident and take any necessary steps to prevent recurrence
- report to all affected parties and maintain communication and confidentiality throughout investigation of the incident
- identify problems caused as a result of the incident and to prevent or reduce further impact
- contact 3rd parties to resolve errors/faults in software and to liaise with the relevant service and departmental personnel to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other systems and services
- ensure all system logs and records are securely maintained and available to authorised personnel when required
- ensure only authorised personnel have access to systems and data
- ensure all documentation and notes are accurately maintained and recorded in Service Manager and made available to relevant authorised personnel

Where appropriate, Incidents can be presented to the Operations Board via departmental representatives and may be included on the log.

All incidents logged within Service Manager shall have all the details of the incident recorded – including any action/resolution, links or connections to other known incidents. Incidents which were initially resolved but have recurred will be reopened or a new call referencing the previous one will be created.

Monthly reports on incidents generated by the Service Manager system are automatically sent to the Information Security Manager to facilitate the monitoring of the types, numbers, frequency and severity of incidents which will help to correct and prevent incidents recurring.

During the course of incident investigations, hardware, logs and records may be analysed by Allocates internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential during the course of these investigations that confidentiality is maintained at all times.

The Information Security Manager is initially responsible for handling security incidents and will make a decision as to whether an incident needs to be "handed" over and dealt with (including closed) by departmental representatives where appropriate.

Policy Governance

The following table identifies who within Allocate Software plc. Is Accountable, Responsible, Informed or Consulted with regards to this policy.

The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.
- Accountable – the person who has ultimate accountability and authority for the policy.
- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Operations Director
Accountable	ISMS Manager
Consulted	Allocate Software Operations Board
Informed	All Staff

Allocate Software Ltd
Corporate and UK head office
1 Church Road
Richmond
TW9 2QE
UK
Tel. +44 (0)20 7355 5555

Allocate Software AB
Sweden office
Box 30077
104 25 Stockholm
Visiting address:
Franzéngatan 3
112 51,
Stockholm, Sweden
Tel. +46 (0)8 50551800

Allocate Software GmbH
Germany office
Ruhrallee 9
44139 Dortmund
Germany
Tel. +49 (231) 9525211

Allocate Software PTY Ltd
Australia head office
Suite 2, Level 13
99 Mount St
North Sydney
NSW 2060
Australia
Tel. +61 (0)3 9534 4477

Allocate Software España SL
Spain office
Avda. de Europa 19 3ºA
Parque empresarial La Moraleja
28108 Madrid
Spain
Tel. + 34 91 793 21 00

ALLOCATE