COVID-19 Test Trace, Isolate, Support (TTIS)

CMS Telephony 8x8 (CMST8)

System Security Policy (SSP)

Document control

Title	CMS Telephony (8x8) - CMST8 - System Security Policy (SSP)
Author	NHS National Services Scotland
Creation date	10th June 2020

Version history

Version	Date	Comments
0.1	10th June 2020	Initial Draft
0.2	15th June 2020	Second Draft following call with 8x8 personnel
0.3	20th June 2020	Update following internal Digital and Security Directorate Information Security and Governance review
0.4	26th June 2020	Update following Security and Architecture Review Board (SARB) review
1.0	22nd July 2020	Update to include users who don't work for the NHS login mechanisms. Also version changed to 1.0 as approved by SARB

Table of contents

1 CMS Telephony (8x8) overview

1.1 Introduction

1.1.1 (Name of the system, background high level overview)

1.1.2 The Test-Treat-Isolate-Support (TTIS) programme of work includes multiple new technologies to provide services such as Contact Tracing via the Case Management System (CMS). The CMS SSP provides more detail on why these systems are required and how they interact.

This SSP relates to the use of two 8x8 Inc systems: “Virtual Call Centre” (VCC) and “Virtual Office” (VO), which are integrated with NSS’ ServiceNow to make up the overall CMS solution. This CMS Telephony SSP includes both VCC and VO as a combined system, thereafter referred to as “CMST8”.

The “8x8 Telephony” systems (VCC and VO) provide the telephony capability for Contact Tracers to communicate with patients and citizens (non-patients) who are potentially at risk of suspected disease through contact with someone who may have been at risk of suspected disease.

Communication between contact Tracers and patients or citizens is two-way, through use of outbound and inbound calls.

The VCC contains the Agent Console and Supervisor Console.

1.2 Business goals/benefits of the system

1.2.1 (Purpose of the system, ownership, funding – any risk that might be accepted is accepted to enable the delivery of the business benefits)

1.2.2 The purpose of CMST8 is to enable NHSScotland to contact both patients and citizens (non-patients) to investigate their movements in order to determine which people they have been in contact with. A record of these associated people (contacts) is maintained, for these contacts to then be contacted.

The CMST8 provides no mechanism for direct access by patients or citizens to any component of CMS or TTIS.

Public Health Scotland (PHS) own the overall TTIS service, which utilises a suite of solutions including this Telephony system. Funding is understood to be sourced from Scottish Government.

1.3 System status and timescales

1.3.1 (Current status of system/project, e.g. “outline business case”, “requirements”, “user acceptance testing”, associated timescales)

1.3.2 Due to the perceived urgency to provide a solution, the initial TTIS / CMS systems have been developed quickly with direction from PHS and external consultancies such as Cap Gemini.

As at June 2020, work is currently progressing towards a Minimum Viable Product (MVP), which is expected to be piloted on Mon 15th June 2020, with go-live on Mon 22nd June 2020. Thereafter, further versions will be implemented.

1.4 System security policy statement

1.4.1 "The system shall employ appropriate security controls and manage risk throughout the life of system to ensure the confidentiality, integrity, availability of data and services is protected."

Describe any solution specific objectives, special considerations related to the type of information processed, environment in which system will operate, overview of how it is planned these objectives will be met)

1.4.2 The purpose of the Policy is to protect the information assets from all threats, whether internal or external, deliberate or accidental. The objective of information security is to ensure business operations continue by preventing breaches of security. The system shall employ appropriate security controls and manage risk throughout the life of the system to ensure the confidentiality, integrity, availability of data and services are protected.

As CMST8 gathers some information about patients and citizens, the solution includes a definition of ownership that includes patients and citizen as well as the Parties responsible for technical security and management of information. All Parties will be informed of their duties in respect of maintaining the privacy and integrity of the information within NHSScotland.

CMST8 shall be managed by NHS National Services Scotland, with direct system management delegated to "8x8 Inc", and will include regular maintenance activities, technical support services, test and release services, service performance targets, incident management, problem triage and resolution, service reporting and escalation.

The core cloud platform is subject to bi-annual security penetration test by an independent external accredited security organisation. Identified security threats shall be assessed by the System Owner and System Operator and if required a remediation plan shall be prepared and executed, and re-testing carried out by agreement.

1.5 Privacy impact assessment

1.5.1 (Any solution that processes personally identifiable data or other sensitive data must have a corresponding completed Privacy Impact Assessment. Provide summary of key points and cross reference here)

1.5.2 A “Case Management Service DPIA” is being prepared by the Digital and Security Information Governance team.

1.6 Responsible parties

1.6.1 (Identify individual holders of key roles: system owner, system manager, senior information risk owner (SIRO), Information security officer (ISO), information governance officer, cross reference Appendix B if necessary)

1.6.2 The following individuals are responsible:

- System owner: (who is paying for the system):

  NHS National Services Scotland (NSS) / Scottish Government

- System manager: (who is responsible for implementing/managing the system).

  NSS

- Senior information risk owner (SIRO): (the person ultimately responsible for signing off the risk assessment).

  NSS Digital and Security Director

- Information security officer/Accreditor: (a security practitioner assisting in the development of the risk assessment).

  Information Security Consultant (Information Security and Governance, NSS Digital and Security)

- Information governance officer: (an information governance practitioner assisting, most likely cross referenced to PIA).

  Senior Consultant Information Governance (Information Security and Governance, NSS Digital and Security)

2 System description

2.1 Context

2.1.1 (Describe key information like hosting locations, suppliers, functions, information processed, interdependencies – key points, high level)

2.1.2 The 8x8 Telephony system (CMST8) is a cloud Software as a Service (SaaS) product, which provides functionality to connect a contact tracer with patients / citizens via a Public Service Telephone Network (PSTN). 8x8 Inc offer the option to install a thick-client that provides additional functionality, which will be deployed as default for CMS.

This CMST8 solution is a key component of the TTIS Case Management System, and is interdependent with NSS' ServiceNow CMS solution, which uses the ServiceNow "Customer Service Management" module.

This CMST8 solution will utilise the thick client.

System records, including patient and citizen data, are stored in 8x8's cloud storage.

2.2 Operation

2.2.1 (Brief step by step description of key use cases)

2.2.2 Virology information, received from Laboratory systems (LIMS) via ECOSS, contains results for Patients who have tested positive. This data is on-boarded into CMS with Patient demographic and contact information. If information for a patient already exists, it should be updated.

Users (Contact Tracers) initiate contact with patients from their own NHS Board who have tested positive (index cases). This requires both 8x8 and ServiceNow to be running concurrently. Calls are routed via a Telephone PBX (Private Branch eXchange).

Incoming calls: Passed by the PBX to a Contact Tracer using ServiceNow. The appropriate screen is opened for CTs to enter or update information.

Outgoing calls: initiated by a CT using ServiceNow, 8x8 receives the number via an API call, and the telephone call is then routed through the PBX to the PSTN.

2.3 Hardware

2.3.1 (Architecture, summary of hardware, versions, configuration)

Server hardware is cloud-based.

2.4 Software

2.4.1 (Server OS/platforms, versions of server and client software, thick or thin client, underlying/enabling technologies where appropriate (such as Java, .NET, php, etc.)

2.4.2 As part of CMS, 8x8 runs as Software as a Service (SaaS) using vendor proprietary software. The software is managed and controlled by the vendors and is used globally as a service.

2.5 Interfaces

2.5.1 (List interfaces with other networks/systems/applications/organisations, describe how each communication and interface works e.g. SMTP email, web based access using SSL over HTTP, Internet facing web services based on WSDL, etc. Where possible capture specific technologies and versions of protocols in use)

2.5.2 CMST8 endpoint devices access CMS using a supported browser over HTTPS. For NHS users Azure Active Directory (AAD) will be used for multi factor authentication (MFA) to authorise the user to the CMST8 and ServiceNow systems using the same domain credentials. All other users, as an example Local Authority staff will use local accounts.

2.6 Accreditation scope

2.6.1 (Summarise what is in scope and any scope exclusions)

2.6.2 The accreditation scope covers the CMST8 component, which makes up CMS with ServiceNow:

- 8X8 Virtual Contact Centre/Virtual Office

Exclusions include the parallel and downstream components where data is consumed. For example:

- ServiceNow Case Management Service Module.

1

2.6.3 Figure 1 shows an overview diagram of the system.

*2.6.4 **(Diagram is essential** – logical diagram based on physical locations – initially identify locations as boxes, put system components in each location, describe architecture and connectivity, add interfaces to other systems/networks/applications, place data storage and user groups)*

1

8x8 System Overview

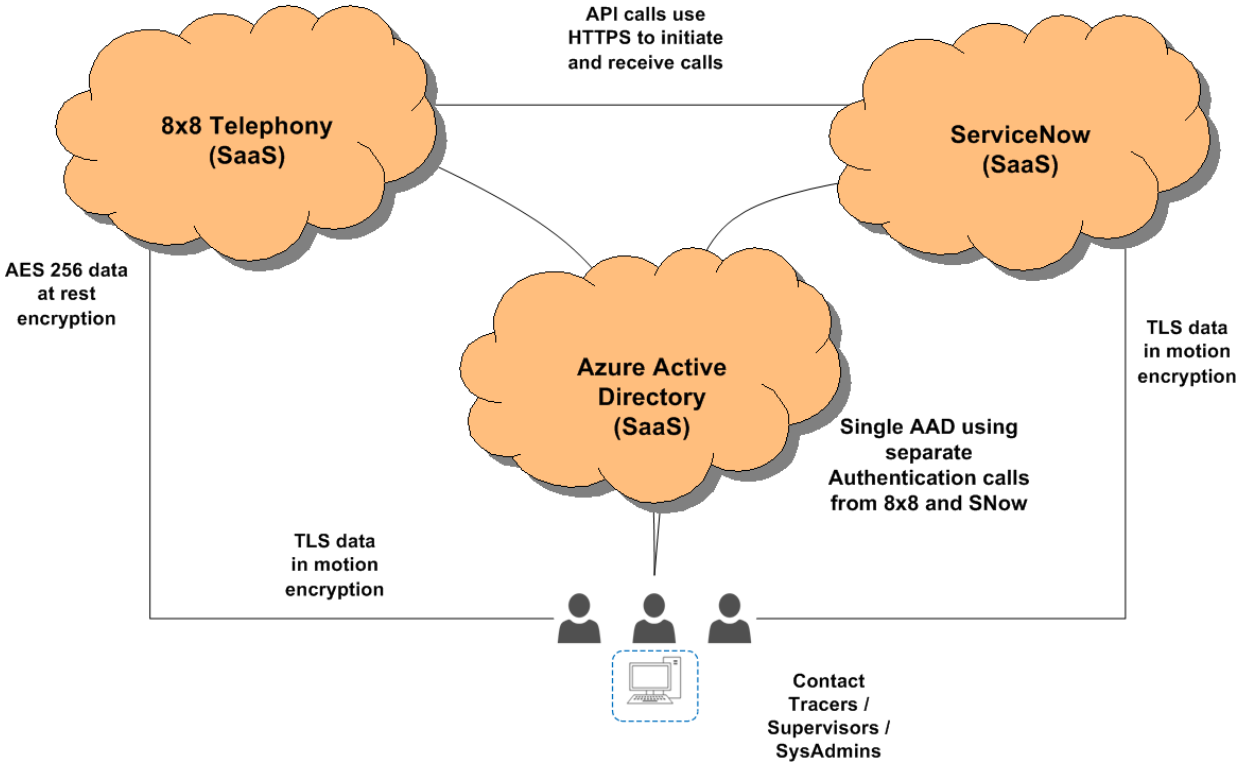

Figure 1: diagram of proposed architecture

3 Assets and services

3.1 Introduction

At the heart of a risk assessment are assets that are valuable to the business and need to be protected – these assets include:

- **Information assets** e.g. NHS data sets that must be protected from risks such as unauthorised access and loss
- **Physical assets** e.g. mobile devices or data centre equipment that must be protected from threats such as theft and fire damage
- **Services** e.g. clinical applications or infrastructure services like AD and DNS that must be protected from threats such as loss of service

This section captures the assets that are to be protected in the case of this information system.

3.2 Information assets

Table 1 lists the information assets

Depending on the type of data, 8x8 determine themselves to be either a Processor, Controller, or “Processor - Access”

ID	Name	Description	NHS sensitivity
A1	Processor: Call Recording	Although 8x8 default configuration is for Call Recording to be switched off, this implementation will be set to ON. Recorded calls can be downloaded by NHS Admins. 8x8 note: “Call Recordings are written to the Virtual Office SAN, encrypted Recordings are retained for the contracted duration + 24 hours, then deleted Deletion utilises standard OS level delete commands Any residue data on disc after deletion is overwritten via natural disc re-use”	Amber
A2	Controller: Call Data Records (or CDRs)	Call logs	Green

Table 4: information assets

8x8 Inc note:

“The Scottish Government tenant will be built on at least 2 UK data centres at any one time and will be replicated at further data centres in the event of an issue at any single site providing N+1 resilience at all times. We have 4 geographically separated, Tier 3, UK data centres. The Public Health Scotland service would be based on this UK based, Government cluster, alongside our UK Government and Local Government clients. All Public Health Scotland client data will be stored within these UK Data Centres initially before being transferred to NSS. 8x8 will thereafter delete their copy of the client data.

All 8x8 staff involved with our UK Government contracts have Government security clearance Up to Baseline Personnel Security Standard (BPSS). SC clearance has been obtained for key personnel engaged in our OFFICIAL networks.”

Processor: “Data that is provided to 8x8 for 8x8 to process on their behalf, including data that constitutes personal data whereby 8x8 acts in its capacity as a processor, such as VCC Configuration, PBX and all 'Customer Content' data will reside within the United Kingdom.”

Controller:

“Data generated by the 8x8 systems, and user license data, may be stored, accessed and used outside the UK by our parent company, 8x8, Inc”

(Quoted extracts above from “UK Customer Deployments Data Safeguards 17 June 2019.pptx” and “8x8 Security Statement.pdf”)

The “NHS sensitivity” is the label applied to the information according to the NHS Scotland traffic light system as set out in Table 2.

Label	Description
Green	This is information which is unlikely to cause distress to individuals, breach confidence or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person’s name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person’s physical or mental state.
Amber	In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular: • any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost. • any information which if lost or disclosed to unintended recipients would lead to a low risk to a person’s safety (e.g. loss of an address but no evidence to suggest direct harm would result). • any information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments).

Label	Description
Red	Most boards also hold some information which is highly sensitive. Particularly: • Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way). • Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health. • Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file). • Information relating to vulnerable persons' health (e.g. child protection cases) • Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment). • Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Table 6: NHS Scotland traffic light sensitivity descriptions

3.3 Physical assets

Table 3 lists the *major* physical assets comprising the system. (If it is a managed service and the supplier owns all the major physical assets this section can be omitted)

Section omitted on basis that NHSS do not own or provide any hardware for operation of 8x8 technologies.

ID	Description (model, type, configuration for all of these)	Cost to replace
PA1	None as supplier owns and manages all major physical assets	
PA2		
PA3		

Table 8: physical assets

3.4 Services

Table 4 lists the services provided by the solution.

ID	Name	Description	Max. tolerable downtime
S1	8x8 Telephony	Cloud based telephony service "Our Cloud service is based upon a distributed data centre model and we currently operate 15 data centres world-wide, four of which are in the UK. We have a platform uptime of 99.999% with un-planned service downtime of <1 minute per year. We offer Customers a service availability of 99.99%."	0.5 day
S2			
S3			

Table 10: services

4 People

4.1 User groups

4.1.1 Table 5 lists the user groups with access to the system.

ID	Name	Description	Type of access	Number[1]
U1	Contact Tracers	NHS Staff who communicate with patients and citizens	Update	1000>9999
U2	Contact Tracers Supervisors	NHS Staff who manage Contact Tracers	Update	100>999
U3	CMS Administrators	Administrators manage the 8x8 configuration and RBAC	Access Control	10>99
U4	8x8 Inc	supplier support	Full	10>99

Table 12: User groups

4.1.2 In addition to people based sources of threat the following non-people based sources of threat should be considered in the risk assessment:

4.2 Other sources of threat

4.2.1 In addition to people based sources of threat the following non-people based sources of threat shall be considered in the risk assessment:

- Environmental threats such as fire, flood
- Technical threats such as technical failure of equipment
- Automated threats such as worms that propagate mostly without human interaction

[1] Approximate number band: 1-9, 10-99, 100-999, etc.

5 Security controls

5.1 Supplier arrangements

5.1.1 What suppliers are involved in provision of any aspect of the solution? (identify all supplier groups including internal/health board teams, and external commercial third parties)

5.1.2 8x8 provide and manage the Telephony system and associated cloud storage services.

8x8 have issued details for NSS and / or NHS Boards to provide the appropriate local infrastructure for Contact Tracers to operate VCC&VO.

5.1.3 What contracts are in place? Summarise the information security/information governance/data protection contract terms, or other arrangements.

5.1.4 8x8 issued a Contract Proposal, dated 3rd June 2020, details of which are available on request.

5.1.5 Do information security requirements that apply to the named contractor also apply to any subcontractors? Name any sub contractors.

5.1.6 No third-party subcontractors are used; only 8x8 Inc's own employees.

5.1.7 Who is responsible for reviewing supplier performance and ensuring conformance with security requirements?

5.1.8 Performance by NSS; Security by Information Security and Governance, NSS Digital and Security team.

5.1.9 What independent assurance/audits/certifications are applicable to any part of the solution? Describe the scope of any applicable certifications.

5.1.10 ISO27001:2013; Cyber Essentials Plus; "Her Majesty's Government Authority to Operate"; HIPAA; FISMA; "Cloud Security Alliance";
Datacentre security standards: Complies with a recognised standard CSA CCM version 3.0

5.2 Access control

5.2.1 How are new users provisioned? How is it ensured that users get the correct permissions?

5.2.2 Access is managed by NSS Administrators. Following Azure Active Directory integration, these will be provisioned through Active Directory groups. Users working on behalf of Health Boards (as an example, Local Authorities) are provisioned with local user accounts, these users invariably do not exist within participating boards active directory therefore local accounts are required.

RBAC is employed to make sure authenticated users are assigned the correct role with the appropriate permissions.

5.2.3 How do users log onto the solution? Are there different options for different interfaces?

5.2.4 NHS users will login using either username / password or Active Directory credentials. Users working on behalf of Health Boards (as an example, Local Authorities) are provisioned with local user accounts, these users invariably do not exist within participating boards active directory therefore local accounts are required.

5.2.5 How is it ensured that users can only access the information and functions for which they are authorised?

5.2.6 8x8 Inc note: "All applications provided come with role-based access controls. These are initially configured during the deployment phase and can thereafter be administered by Customer senior administrators via the configuration tools. All Admin changes are logged.

All data centres deployed in the solution employ Physical Access Controls complying with CCM v3.0 and SSAE-16 / ISAE 3402

All Admin access is logged and recorded and is auditable."

5.2.7 How are the user accounts managed? For example who removes accounts of staff that leave the organisation, resets forgotten passwords, updates a users permissions, changes to permissions, etc?

5.2.8 NSS Admin users will undertake provision and management of new accounts for Contact Tracers.

5.2.9 How can users recover their account if they forget their credentials?

5.2.10 Account management and recovery is controlled through normal BAU processes. The specific method is dependent on the access method for the Contact Tracer, either:

- via a password-reset email to the user's email address, or
- through Active Directory.

5.2.11 How are user credentials, such as passwords, stored within the system?

5.2.12 Until all NHS organisations are able to use AAD, this is dependent on the access method for each Contact Tracer, either:

- username / password are stored using salted hashed passwords, or
- Authentication via Active Directory

When all NHS organisations are authenticating via Active Directory, passwords will not be stored within 8x8 systems. No 8x8 passwords are stored in ServiceNow.

5.2.13 Are any individuals/groups, who are **not** authorised users of the system, able to access any part of the system e.g. the hardware or shared infrastructure components? (For example cleaners or patients that may be able to access physical terminals in shared areas; or users of other applications that may be able to access a shared database or hosting environment)

5.2.14 No.

5.3 Personnel controls

5.3.1 What personnel pre-employment screening checks are applied for personnel involved in provision of the service?

5.3.2 8x8 personnel controls: “All 8x8 staff involved with our UK Government contracts have Government security clearance Up to Baseline Personnel Security Standard (BPSS). SC clearance has been obtained for key personnel engaged in our OFFICIAL networks. NPPV clearance is available for staff working unaccompanied at Police or Fire Service sites if required.”

5.3.3 How are users made aware of their security responsibilities with respect to the system? (e.g. to keep their password secret, or to report a security breach?)

5.3.4 Tracking and tracing/Call handlers: Users of this application are already subject to training on information safe handling. The use of this application falls within the scope of their existing briefings and training and includes, clear communication of acceptable use policy, security of information systems and code of compliance.

5.3.5 What training is provided to system administrators or managers on how to properly run the system?

5.3.6 Managers of CMS follow clear procedural guidance set out as part of security awareness training. This training is subject to periodic review and captured as part of Cyber Essentials.

5.3.7 What information security and governance training is provided to users of the system?

5.3.8 NHS employees are subject to security awareness training and information safe handling within the NHS. This application falls within the scope of their existing briefings and training on the secure use of information systems.

5.4 Network security controls

5.4.1 Are the system's network interfaces hardened? For example have all unnecessary services been disabled and ports closed?

5.4.2 Yes. 8x8 is a cloud based SaaS platform subject to a number of security controls, namely, DDoS prevention, annual pen testing, vulnerability scanning, firewalls, Anti-virus.

"Service Organization Control (SOC) reports: 8x8's information security control environment applicable to the Services undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 audits.

Additionally, the Covered Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis."

5.4.3 How does the solution protect access to network traffic on shared networks?

5.4.4 The solution is deployed within public cloud where it does not have any access to network traffic on shared networks.

5.4.5 How is the hosting environment separated/protected from connected networks (e.g. firewall(s), models, config, etc.)?

5.4.6 Cloud SaaS services provide this protection by default

5.4.7 Have all network components been deployed in a hardened configuration, for example all default passwords changed, and unneeded services blocked?

5.4.8 Yes – see note above re "Service Organisation Control (SOC) reports"

5.4.9 Is the solution remotely accessible? If so, how is the remote access provided and controlled?

5.4.10 The solution is a public cloud based SaaS Multi Factor Authentication (MFA) is deployed as a security control. Administrator access is via cloud management portal. MFA access is strictly controlled with only those permissions required to carry out infrastructure maintenance being granted with role-based access control and under change control agree by the relevant CAB.

5.5 Data protection

5.5.1 Who are the data controllers and data processors for this solution?

5.5.2 NSS, as a Data Controller will operate the service on behalf of NHSScotland Boards.

See Table 1: information assets for additional information on 8x8 Inc's statement.

5.5.3 Are all information assets held in the system allocated to a responsible owner?

5.5.4 Yes, details of the Data Controllers and Data Processors are detailed in the DPIA.

5.5.5 Are any technical controls employed within the solution to protect information assets? For example encryption at rest, de-identification or data obfuscation.

5.5.6 All information assets within the 8x8 solution are protected using AES 256 data at rest encryption, and the latest version of TLS data in motion encryption.

Data Encryption in Transit: "8x8 data is encrypted both in motion and at rest.

Data Encryption at Rest: "FIPS 140-2
8x8 utilises Vendor provided encryption solutions which comply with the US FIPS 140-2 standards as a minimum. Details of the FIPs compliance process is available here[2]"

5.5.7 What controls are in place to ensure secure disposal of hardware and information assets? For example to prevent unauthorised recovery of data on recycled hard disks, or secure shredding of printed output.

5.5.8 After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

"**Data sanitisation type**: Explicit overwriting of storage before reallocation; Deleted data can't be directly accessed; Hardware containing data is completely destroyed.

Equipment disposal approach: Complying with a recognised standard, for example CSA CCM v.30, CAS (Sanitisation) or ISO/IEC 27001"

5.5.9 How is data imported/exported from the solution? What controls are employed to protect any data on removable media?

5.5.10 There is no data import/export to/from the SaaS solution.

5.5.11 What information transfers does the solution permit/enable? How are these controlled?

5.5.12 There is no data transfer to/from the SaaS solution, however it is possible for a call recording to be downloaded from a secure cloud area using secure file transfer to NHS storage if required e.g. for an investigation.

5.6 Physical and environmental security

5.6.1 What physical or environmental controls apply at any locations where the solution is hosted?

5.6.2 All 8x8 Cloud-based data centres deployed in the solution employ Physical Access Controls complying with CCM v3.0 and SSAE-16 / ISAE 3402

5.6.3 What physical security controls apply at any locations from where the solution is used/accessed?

5.6.4 Public Cloud providers physical security policy applies to all forms of physical security including:

- multi-zone security
- man-traps
- appropriate perimeter deterrents (fencing, berms, guarded gates)
- on-site guards
- biometric controls
- CCTV
- secure cages
- fire detection and fire suppression systems both localized and throughout the data centre floor.

Participating NHS boards' local physical security policy should apply.

Participating NHS Boards' computers used by staff are protected by standard security measures governed by local security policy.

5.7 Operational security

5.7.1 Who is responsible for Information Backup controls? Describe the data backup and recovery process.

5.7.2 Platform backup is the responsibility of 8X8 as part of the SaaS. With regards recovery, a support ticket would be raised to recover the service from backup.

8x8 Inc note: "By selecting 8x8's proposed cloud services, you will automatically benefit from the inherent business continuity and disaster recovery that cloud services offer.

Our Architecture is described below and has inherent N+1 resilience throughout. We connect to 26 global tier 1 carriers worldwide and 7 in the UK providing resilience in terms of our PSTN and SIP connectivity.

From a Business continuity perspective our business, core applications and those of our partners are all cloud based and can therefore be accessed from any Internet connected location

At any one time, three database replicas are running—one primary replica and two or more secondary replicas. If the hardware fails on the primary replica, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, a new replica is automatically created. So, there are always at minimum two physical, consistent copies of our customers' data in the datacentre. Application servers are also automatically replicated to protect customers of failure of an individual server."

5.7.3 Who is responsible for solution Change Management? Describe the change management process.

5.7.4 Process: "8x8 operate Change Management Process in line with ITIL guidelines. 8x8 solutions are tested prior to being brought into service in accordance with pre-agreed test plans, which vary by solution. All planned changes go through a CAB process and risk assessment. Roll back plans are evaluated prior to approval of a change.

The deployment will follow the 8x8 Release and Deployment process, following review and authorisation via the Change Management process

As a SaaS provider we schedule service releases once per quarter. All releases will go through the 8x8 CAB and will be notified to the customer in advance of deployment. Our updates are not service affecting."

5.7.5 What anti-malware controls apply within the solution?

5.7.6 Full provision included as part of SOC accreditation

5.7.7 How are information security incidents (or potential information security incidents) reported, managed and communicated?

5.7.8 This is performed through NSS normal procedure using the online ServiceNow incident reporting tool. The members of the ServiceNow security group monitor, analyse and respond to security incidents following their standard operating procedure. Depending on the nature of the incident, the ServiceNow security group will escalate and engage response teams necessary to address an incident reported to NSS Security Team.

All events and suspect events that could result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems must be reported immediately.

- Name of person reporting the incident

- The type of data or information involved (be it electronic or physical)
- Whether the loss of the data puts any personal or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of information or equipment affected
- Type and circumstances of the incident

8x8 note: “Incident Management: 8x8 maintains security incident management policies and procedures. 8x8 notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by 8x8 or its agents of which 8x8 becomes aware to the extent permitted by law.”

With any or potential information security incident, the immediate obligation is to the NSS Adverse Events Management Policy and QPulse.

Incident Response and Resolutions Times

The Services will be provided with Incident Call Response Times and Resolution Times meeting or being less than the maximums in the following table:

Incident Level	Maximum Call Response Time	Maximum Resolution Time	Summary
Severity 1	30 Minutes	24 Hours	8x8 will work 24/7 to restore service
Severity 2	30 minutes	24 Hours	8x8 will use commercially reasonable efforts to restore efforts
Severity 3	1 Hour	72 Hours	8x8 will use commercially reasonable efforts to restore efforts
Severity 4	1 Hour	Variable	

Further information on 8x8 responsibilities is detailed in their contractual documentation.

5.7.9 What controls have been employed to ensure continuity of service?

8X8 SaaS solution is a global highly available system.

5.7.10 Has a business continuity plan and a disaster recovery plan been produced for the solution? Have these plans been tested?

5.7.11 8x8 “maintain a BCDR plan that supports the loss of our Customer Support, Network Operations Centre, Security Operations Centre and UK HQ sites as

well as the loss of a single, or multiple data centres. We test our BCDR and Failover capabilities annually and our data centre failover capability every 6 months."

8x8's BC/DR plan states:

Their architecture "has inherent N+1 resilience throughout", connecting to "26 global tier 1 carriers worldwide and 7 in the UK providing resilience in terms of their PSTN and SIP connectivity".

Their "business, core applications and those of our partners are all cloud based and can therefore be accessed from any Internet connected location".

"At any one time, three database replicas are running—one primary replica and two or more secondary replicas. If the hardware fails on the primary replica, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, a new replica is automatically created. So, there are always at minimum two physical, consistent copies of our customers' data in the datacentre. Application servers are also automatically replicated to protect customers of failure of an individual server."

"Call Forwarding in Disaster situations: In the event that a Customer site is not operational or has to be evacuated at short notice, If it is necessary to forward calls to an alternative location during either business as usual operation or a local loss in service, this can be performed manually or automatically based on predefined triggers within the call queue scripting."

5.8 Audit controls

5.8.1 Describe the audit controls employed by the solution. What events are recorded? For how long are audit logs retained? What tools are available to analyse audit logs?

5.8.2 8x8's Security Policies and Procedures:

The 8x8 Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash. Following Azure Active Directory integration, passwords will neither be logged nor stored.
- User access log entries will be maintained, containing date, time, user ID, URL executed, or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, 8x8 can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis

- Certain administrative changes to the Services (such as adding custom fields) are tracked and are available for viewing by a customer's system administrator. Customers may download and store this data locally.

5.8.3 Who is responsible for auditing system access?

5.8.4 Audit logs are available to NSS Admins

5.8.5 How are audit logs protected from unauthorised access or modification?

5.8.6 Data Centre physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.

5.9 Solution development, testing and maintenance

5.9.1 Who is responsible for deploying patches and updates?

5.9.2 8x8 Inc

5.9.3 In what timescales will patches and updates be deployed?

5.9.4 SaaS offers daily vulnerability scanning any vulnerabilities detected are remediated as part of the managed service.

In addition, 8x8's Change Management Process notes:

"8x8 operate Change Management Process in line with ITIL guidelines. 8x8 solutions are tested prior to being brought into service in accordance with pre-agreed test plans, which vary by solution. All planned changes go through a CAB process and risk assessment. Roll back plans are evaluated prior to approval of a change.

The deployment will follow the 8x8 Release and Deployment process, following review and authorisation via the Change Management process

As a SaaS provider we schedule service releases once per quarter. All releases will go through the 8x8 CAB and will be notified to the customer in advance of deployment. Our updates are not service affecting."

5.9.5 Are any components of the solution **excluded** from the above patching policy?

5.9.6 No

5.9.7 Describe the patch deployment process.

5.9.8 8x8 Inc note:

"8x8 assesses potential threats to our service using top-rated vulnerability scanning tools.

The speed of patch deployment depends on the criticality. If 8x8 deems it high priority, 8x8 addresses it immediately. If medium priority, within a week. If low, within two weeks.

5.9.9 What testing controls are in place to understand any potential unintended impacts of updates?

5.9.10 The cloud SaaS providers make Dev, Test and Live platforms available for regulated testing controls.

5.9.11 What agreements are in place to ensure the solution keeps pace with information security developments? For example migrating onto new information technologies when previous versions become obsolete/unsupported.

5.9.12 The solution is cloud-based SaaS, therefore security updates are included as part of the managed service provided by 8x8.

5.9.13 What security or vulnerability tests have been performed on the solution? What was the outcome of the test? What commitment has been made to ongoing security testing?

5.9.14 PEN testing is performed by a third party on a bi-annual basis, this along with the daily vulnerability scanning helps identify risks and remediation that increase security of the managed service.

5.9.15 Is there a separate test and development environment? Is any live data utilised in this environment? How is access to the test and development environment controlled?

5.9.16 Yes, there are separate test and development environments. No live data is used in any of the test or development environments.

5.10 Assumptions

5.10.1 What assumptions have been made about security controls that are out of scope of this SSP? For example assumptions about controls that are believed to be the responsibility of the health boards or suppliers such as end user device security, behaviours or responsibilities, physical/environmental security at operating locations, etc.

5.10.2 It is assumed that:

- the physical and environmental security of the public cloud data centres is the responsibility of the SaaS provider and is out of scope for this SSP
- the security of end user devices used to access the solution are the responsibility of the end user and is out of scope for this SSP

6 Risk analysis and recommendations

This section to be completed in collaboration with the Accreditor/information security practitioner.

6.1 Risk appetite guidance

6.2 A risk appetite provides a guideline for what action should be taken in response to an identified risk.

6.3 The risk appetite of NHS organisations is typically "cautious" and is represented in the table below. This provides an indication of appropriate response to risk.

Extreme	**20-25**	**Unacceptable level of risk exposure that requires immediate corrective action to be taken, and monitoring at Executive and Board level.**
Major	15-19	Unacceptable level of risk which requires measures be put in place to reduce exposure, and monitoring at Executive and Board level,
	10-14	Unacceptable level of risk exposure that requires measures be put in place to reduce exposure and monitoring at Executive level and potentially Board level
Moderate	8 or 9	Acceptable level of risk exposure subject to regular active monitoring measures by senior managers.
Minor or Negligible	1-7	Acceptable level of risk subject to regular passive monitoring measures at local management level.

Table 15: NHS Scotland Risk appetite guideline

6.4 Residual risk statement

6.4.1 No significant residual risk

6.5 Risk treatment recommendations

6.5.1 Significant residual risks

- No significant residual risks identified within the solution.

6.5.2 Risk treatment

- Information Security and Governance, NSS Digital and Security recommend bi-annual review of system administration processes and procedures as best practice.

6.5.3 Accreditation recommendation

- Information Security and Governance, NSS Digital and Security recommend approval of this SSP.

6.5.4 System Security Policy approved.

7 Annex A – NHS Scotland risk matrices

7.1 Impact/consequence definitions

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Patient Experience	Reduced quality of patient experience/clinical outcome not directly related to delivery of clinical care.	Unsatisfactory patient experience/ clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience/ clinical outcome; short term effects – expect recovery <1wk.	Unsatisfactory patient experience/ clinical outcome; long term effects – expect recovery >1wk.	Unsatisfactory patient experience/ clinical outcome; continued ongoing long term effects
Objectives / Project	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over-run.	Inability to meet project objectives; reputation of the organisation seriously damaged.
Injury (physical and psychological) to patient/visitor/staff.	Adverse event leading to minor injury not requiring first aid.	Minor injury or illness, first aid treatment required.	Agency reportable, e.g. Police (violent and aggressive acts). Significant injury requiring medical treatment and/or counselling.	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity
Complaints / Claims	Locally resolved verbal complaint.	Justified written complaint peripheral to clinical care.	Below excess claim. Justified complaint involving lack of appropriate care.	Claim above excess level. Multiple justified complaints.	Multiple claims or single major claim Complex justified complaint.
Service / Business Interruption	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service.	Short term disruption to service with minor impact on patient care.	Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service.	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core service or facility. Disruption to facility leading to significant “knock on” effect

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Staffing and Competence	Short term low staffing level temporarily reduces service quality (< 1 day). Short term low staffing level (>1 day), where there is no disruption to patient care.	Ongoing low staffing level reduces service quality Minor error due to ineffective training/implementation of training.	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training/implementation of training. Ongoing problems with staffing levels.	Uncertain delivery of key objective/ service due to lack of staff. Major error due to ineffective training/implementation of training.	Non-delivery of key objective/service due to lack of staff. Loss of key staff. Critical error due to ineffectivetraining/ implementation of training.
Financial (including damage / loss / fraud)	Negligible organisational/personal financial loss. (£<1k). (NB. please adjust for context)	Minor organisational/personal financial loss (£1-10k).	Significant organisational/personal financial loss (£10-100k)	Major organisational/personal financial loss (£100k-1m).	Severe organisational/personal financial loss (£>1m).
Inspection / Audit	Small number of recommendations which focus on minor quality improvement issues.	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action. Low rating. Critical report.	Prosecution. Zero rating. Severely critical report
Adverse Publicity / Reputation	Rumours, no media coverage. Little effect on staff morale.	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale/public attitudes.	Local media – long-term adverse publicity. Significant effect on staff morale and public perception of the organisation	National media/adverse publicity, less than 3 days. Public confidence in the organisation undermined. Use of services affected.	National/international media/adverse publicity, more than 3 days. MSP/MP concern (Questions in Parliament). Court Enforcement. Public Inquiry/ FAI.

Table 17: Impact/consequence definitions

7.2 Likelihood definitions

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Probability	Rare - can't believe this event would happen – will only happen in exceptional circumstances	Unlikely - not expected to happen but definite potential exists – unlikely to occur.	Possible - may occur occasionally, has happened before on occasions – reasonable chance of occurring	Likely - strong possibility that this could occur – likely to occur	Almost certain - this is expected to occur frequently / in most circumstances – more likely to occur than not

Table 19: Likelihood definitions

7.3 Risk matrix

	Impact				
Likelihood	**Very low (1)**	**Low (2)**	**Medium (3)**	**High (4)**	**Very high (5)**
Very low (1)	Low1	Low 2	Low 3	Medium	Medium
Low (2)	Low	Medium	Medium	Medium	High
Medium (3)	Low	Medium	High	High	High
High (4)	Medium	Medium	High	High	Very High
Very high (5)	Medium	High	High	Very High	Very High

Table 21: Risk evaluation matrix

7.4 NHS Scotland risk appetite statement

NHS Scotland risk appetite is broadly defined as “cautious”: Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward. Further guidance on the acceptance of risk is defined based on residual risk values:

Residual risk value	1-3	4-8	9-19	20+
	Risk acceptable	Risk may be acceptable if all methods for further mitigating or avoiding the risk have been considered	Further reduction of risk strongly recommended	Risk unacceptable

Table 23: Residual risk statement options