CASELINES SECURITY OVERVIEW

OVERVIEW

CaseLines is a highly secure cloud based system for storage of highly sensitive trial evidence, including material for crimes of sexual violence and also child protection and child abuse cases. The system is certified to ISO 27001 and has been independently assessed to be compliant with CJIS requirements in the US. A SOC 2 Type 2 report can be made available on request to existing customers under NDA. CaseLines has been used by the UK Ministry of Justice since 2015, during which time the system has been approved by the InfoSec function and also successfully passed an independent code inspection commissioned by the MoJ. CaseLines is subject to annual penetration tests by an independent test organisation, and any security vulnerabilities. There are presently no known material vulnerabilities. The CaseLines approach to security is detailed below.

DATA IN TRANSIT PROTECTION

Data is encrypted in transit to ensure data transiting networks should be adequately protected against tampering and eavesdropping. All connections to the server are via TLS1.2 encryption.

ASSET PROTECTION AND RESILIENCE

CaseLines is hosted on Microsoft Azure. All data is stored in a Microsoft Azure Tier 4 data centre accredited to ISO 27001:2013, ISO 27018:2014, AICPA SOC1, AICPA SOC2 & AICPA SOC3. Microsoft handles its own security of its data centres and Microsoft Azure is widely regarded as the most secure data centre available globally.

Additionally, Microsoft has had their data centre physical security measures and protections certified against the CSA Cloud Control Matrix v3.0.1.

As part of our commitment to security of data for our customers, customer data is protected when stored on any type of media or storage within a service to ensure that it is not accessible by local unauthorised parties. All data is encrypted at rest using AES-256 bit encryption.

Additionally, Microsoft Azure data centers employ physical security controls to protect data at rest within the service. The physical access controls used by Microsoft are backed by CSA CCM v3.0.1 certification.

To ensure that the process of provisioning, migrating, and de-provisioning resources does not result in unauthorised access to customer data, customer data is erased when:

- resources are moved or re-provisioned
- a customer terminates their contract with CaseLines
- a customer requests their data to be erased

Microsoft is responsible for the handling of storage media which has held your data. This is the nature of Platform-as-a-Service (PaaS). The storage media is either sanitised or securely destroyed at the end of its life in line with Microsoft's own policies and practices certified against CSA CCM v3.0.1.

Our approach to data at rest protection, specifically encrypting your data to AES256 encryption, ensures that reallocated storage will never contain cleartext data. Finally, customers can be confident that the availability commitments of the service, including the ability to recover from outages, meet their business needs. CaseLines has an SLA in place with commitments from Microsoft to:

- provide 99.95% availability of web applications
- respond within agreed timescales to incidents of their corresponding severity

SEPARATION BETWEEN CONSUMERS

Logical separation between customer data and other customers within the environment is applied to prevent a malicious or compromised customer from affecting the service or data.

In line with our ISO27001 policies, compliance of which is independently audited by BSI, CaseLines undergoes annual penetration tests from an external company to ensure that our security controls have been configured in accordance with good practice when it comes to preventing malicious or compromised customers affecting the CaseLines service or customer data.

Penetration testing allows us to be sure there are no common or publicly known vulnerabilities in the tested components.

Quick and proper implementation of system enhancements based on weaknesses identified via penetration testing is a part of our ISO27001 policy. When designing and adding new features security is a key consideration. The system architecture is designed with protection of customer data at the forefront of design specification.

The company that performs our penetration testing, Context IS, is a member of the following schemes:

- NCSC Cyber Incident Response (CIR) scheme
- Cyber Essentials scheme
- CREST
- CREST STAR
- CBEST
- CTAS

Context IS is also accredited with the following certifications:

- ISO9001:2015

- ISO27001:2013
- FIRST
- Certified Cyber Security Consultancy (CCSC) Scheme

GOVERNANCE FRAMEWORK

Netmaster Solutions employs the use of a security governance framework with policies to govern key aspects of information security relevant to our service.

Netmaster Solutions Ltd is ISO27001 certified. Part of our ISO27001 policy includes an information security management system (ISMS). Our ISMS framework consists of policies and procedures that include all legal, physical and technical controls involved in the organisation's information risk management processes.

Netmaster Solutions runs an Information Security Forum on a regular basis to:

- discuss and review our ISO27001 policies
- identify new risks to information security
- document steps taken to mitigate identified risks to information security
- remain compliant with latest regulations
- ensure continual improvement of information security processes
- keep the company board informed of risks

OPERATIONAL SECURITY

CaseLines applies processes and procedures to ensure the operational security of the service. The service is operated and managed securely in order to impede, detect, or prevent attacks against it.

Configuration and change management controls are applied to ensure that changes to the system do not unexpectedly alter security properties and have been properly tested and authorised and approved by the Change Advisory Board.

All customers are on a continuous upgrade path and always have access to the latest version of CaseLines. Release notes are available on our support desk and product feature announcements are issued via the CaseLines website whenever a major feature is released.

Customers can submit feedback and suggestions for enhancements through appropriate channels such as through the client services department which will then be taken into consideration and placed into the development roadmap if approved.

The CaseLines product team, in line with our ISO27001 policies, follows the Microsoft Security Development Lifecycle and performs impact assessments when considering changes to the software. Possible impact to security of the system is assessed with each change. All changes go through extensive quality assurance (QA) cycles in keeping with Agile development processes before they are released to our customers.

As a cloud based SaaS application, customers are not responsible for undertaking testing, approving system changes, change management or release management. To ensure continuous vulnerability management, CaseLines takes advantage of Microsoft Azure Platform-as-a-Service (PaaS) features. As such Microsoft is responsible for vulnerability management of the cloud platform with policies backed up by certifications in ISO27001 and CSA CCM v3.0.1.
Vulnerabilities identified are patched by Microsoft. The Microsoft Security Bulletin Severity Rating System is specifically referenced by the UK NCSC cloud security principles as one of the recognised models for vulnerability scoring systems.

Microsoft is also responsible for protective monitoring of the cloud platform. Microsoft adheres to extensive proactive monitoring policies backed up by certifications in ISO27001 and CSA CCM v3.0.1.

PERSONNEL SECURITY

CaseLines staff are be subject to personnel security screening and security education for their role.

The provider of the CaseLines solution, Netmaster Solutions Ltd, a Thomson Reuters subsidiary, is BSI accredited to ISO27001 for Information Security Management.

As part of our ISO27001 policy all employees, contractors and sub-contractors are subject to Baseline Personnel Security Standard ("BPSS") check before gaining access to any Netmaster Solutions systems containing customer data. This check conforms to BS 7858: 2012 standards.

Additionally all employees are required to undergo Information Security training on the first day of their employment with Netmaster Solutions before they are granted access to systems containing customer data.
Information Security lectures are given to all personnel on a bi-monthly basis to reinforce ISO27001 policies and provide continual training.
All employee access privileges to CaseLines and to systems used by Netmaster Solutions are recorded and maintained through use of an access control policy.
Access permissions can only be granted after permission has been given through use an access control workflow.
Each request is assessed to determine if the individual requires access before access is granted. Access to systems containing customer data are limited to staff who require access in order to carry out their day-to-day activities.

SECURE DEVELOPMENT

CaseLines is developed according to the Microsoft Security Development Lifecycle (SDL) in line with our ISO 27001 policies. The Microsoft SDL is an industry recognised standard of good practice when developing software.

SECURE CONSUMER MANAGEMENT

CaseLines provides customers with the tools required to help them securely manage their service. Upon set up of CaseLines, customers can nominate administrators for their organisation. Administrators can:

- manage the joiners and leavers process for staff registered on CaseLines
- grant/remove administrator privileges for other users belonging to their organisation
- view contractual information such as page quota, contract renewal date, and previous years statistics.

Support requests can be made via email, submitted as a ticket on our helpdesk or via telephone.

CaseLines staff will never grant access to customer data upon request. All access to customer data is managed by the customer themselves through use of CaseLines extensive access controls.
Regular penetration testing ensures there are no known weaknesses within our access controls.

IDENTITY AND AUTHENTICATION

All users on CaseLines are required to login using a username and password.
CaseLines passwords have complexity rules in place to ensure only strong passwords can be used.
Organisations can optionally choose to require:

- two step verification for additional authentication via email link to registered email address each time a user attempts to log into CaseLines
- two factor authentication via SMS each time a user attempts to log into CaseLines

CaseLines also supports Azure Active Directory or, for an additional fee, federating to another authentication scheme, such as a corporate directory, an OAuth or SAML provider.

SECURE SERVICE ADMINISTRATION

CaseLines processes to manage the operational service are designed to mitigate any risk of exploitation that could undermine the security of the service.
The platform and infrastructure is managed by Microsoft with industry best practice controls in place.
Access to CaseLines service resources on Azure can only be granted to users belonging to the Azure Active Directory containing the service subscription.

CaseLines Azure administrators are able to retrieve a list of audit events pertaining to access events including security reports, activity reports and audit reports. These reports include the ability to view users flagged for risks.
Users highlighted as suspicious can be locked out manually and there are controls in place to automatically lock out users when password entry thresholds are exceeded.
All CaseLines Azure administrators are required to log into the Azure portal using two factor authentication to further mitigate risk of service administration.