ABOUT NIMBUS SECURITY

OVERVIEW

Nimbus is a modern web application achieving World's best practice for data and user access security. The security model consists of three levels, physical security, electronic security and user access security. This document briefly describes security measures taken for Nimbus at each level.

PHYSICAL SECURITY

Physical security relates to the location and accessibility of servers hosting Nimbus databases and file stores, and the reliability thereof.

Nimbus web hosts are implemented using privately owned high performance server stacks running in paired secure data centres. These data centres are fully accredited Tier 3 to 4 installations, implementing world class best practices, including multiple redundant independent power supplies, backup power generators, redundant air filtration and cooling systems, rack mounted equipment to ISO standards, with elevated flooring and sophisticated fire detection and suppression systems.

Access to server floors is strictly controlled, and limited to data centre technicians holding pass cards. They are under 24 x 7 internal and external video surveillance and the facilities are monitored by contracted security firms such as Chubb for external physical breaches. Fully escorted access is necessary for both Nimbus technical support staff and engineering support staff.

All Nimbus data stores implement redundant storage volumes and are fully replicated in near enough real time to the paired data centre. To help guard against large scale natural disasters, the paired data centres are physically separated by at least 1,000 km. In Australia, the paired data centres are located in Brisbane and Melbourne and feature 4n+1 data redundancy.

All data centre hardware equipment is monitored around the clock via SNMP (Simple Network Management Protocol) including routers, switches, UPS systems, and servers. The Network Operation Centres also monitor power, environmental factors (such as temperature and humidity), backup generator status, and network connectivity. All critical services/ports used for Nimbus are electronically monitored for unusual activity, including HTTP, SMTP and HTTPS.

Internet connectivity is assured at each data centre via multiple backbones to at least four independent transit IP providers, using Border Gateway Protocol (BGP4) to determine best case routing.

The Nimbus hosting environment is designed to achieve a 99.985% up time. In the event of a data centre down event, the service host can be switched to the paired data centre without any disruption to customer account "AutoMate" data upload and syncing services.

ELECTRONIC SECURITY

Electronic security relates to the privacy and protection of data from unauthorised access. For Practices and Clients where Nimbus is hosting sensitive and confidential data, this is a critical concern.

Nimbus servers are constructed with Windows Server 2012 and SQL Server 2008. The operating system is tightly locked down, achieving necessary levels of compliance when tested with the Microsoft Best Practice Analyser tool. The following points note some of the steps taken to prevent unauthorised access:

- There is no FTP access to the Nimbus hosts, no publisher services enabled and no way to update the server except via a dedicated VPN access link for Nimbus technical support staff. All servers are physically fire walled, behind high performance, state of the art Cisco equipment, with only the absolute minimum inbound ports enabled as required for inbound mail, and HTTPS web access.

- All user communication with Nimbus hosts is via HTTPS secure protocol and SOAP over HTTPS, thus preventing data taps, electronic eavesdropping or data siphoning en-route between user and Nimbus host.

- Server IP addresses are hidden behind the hardware fire wall and the VPN connection terminated at the fire wall. Server VPN login is limited to a single administration account with highest security level rated password, there are no user or guest access accounts. Data centre staff do not have access to this login, and therefore do not have electronic access to either the Nimbus databases or file stores.

- The Nimbus hosts do not permit directory browsing via the web protocol, and all files are hidden behind ASPX pages, thus cannot be directly accessed from the web.

- The Nimbus mail servers implement industry standard blacklist spam supplier avoidance, do not support an HTML mail client, and relay all incoming mail to specified external mail addresses.

- The SQL server for Nimbus hosts use private login and there is no SQL management console provided on the server, effectively limiting access to Nimbus application code and Nimbus technical admin staff via the dedicated VPN.

- Nimbus server infrastructure and low level protocol support is maintained and regularly tested to achieve an "A" level security rating by the well respected and independent Qualsys SSL Labs, which is higher than many common web services from major industry suppliers.

All Practice and Client files hosted on Nimbus servers are encrypted with 128 bit AES, keyed internally to each account, thus files are not readable by Nimbus Technology technical support staff, nor would be readable to any other person gaining authorised or unauthorised access at the server directory level. This is the same encryption level used by the NSA for "Secret" level documents.

Moreover, should a file somehow be exposed to a different Practice account through some unforeseen hardware, database or operating system malfunction, it will not be readable because decryption will fail. Occurrence of a failed decryption is also logged to the management console and technical support are immediately notified.

USER ACCESS SECURITY

User Access Security relates to the controls over Practice and Client login and privacy thereof. In Nimbus this applies to three access points:; the Practice portal, the Client workspace and the Nimbus Management Console.

Each Practice is assigned a unique 128 bit global identifier (GUID), which is effectively allocated randomly, and this is used to encode the URL for both the Practice portal and Client workspace. The latter also being distinguished from the Practice URL. Thus, knowledge of a Practice or Client URL does not provide a URL to any other Practice portal or Client workspace, as the chances of correctly guessing a128 bit number are extremely low.

Furthermore, these URL's are not exposed in the Nimbus Management Console user interface, therefore Nimbus support staff do not have access to the login pages for Practice portals or Client workspace and privacy of URL to the Practice is assured.

In the event that support staff need access to a customer account for support or training purposes, this is handled by using remote screen sharing software such as GotoMeeting, thus the account holder is in control and can monitor all support staff operations.

In the event that a person gains unauthorised knowledge of a Practice's URL, they will still need a valid login and password to obtain account access. All passwords are stored with "one-way" encryption in the Nimbus database, thus even access to the database tables by Nimbus technical support staff cannot yield login credentials.

Nimbus login operates on a self managed basis, which means that Practices are responsible for maintaining their own logins and passwords, and similarly, clients are also responsible for maintaining their logins and passwords to the Client workspace. Because Practices do not and cannot get involved in maintenance of Client logins, and likewise, Nimbus Technology support staff do not and cannot get involved in maintaining Practice logins, privacy of logins is assured.

Nimbus prevents employees and clients from sharing login codes, thus ensuring that all logins are unique within each Practice database. Unique Client login prevents inadvertent access to another Client's files, however, Nimbus does provide Practices with several approaches for grouping Client entities in the Client workspace, should this be desired, based upon underlying Practice Management system data and relationships.

Nimbus implements current industry best practice for password reset via time limited, single use emailed link to a password reset page, with a user selectable option to use two factor authentication via 6 digit SMS passcode.

Nimbus also helps guards against brute force password cracking programs by adding CAPTCHA code data entry authentication after a set number of invalid password attempts.

Controls are available to Nimbus account holders to adjust certain security settings, for example, security over emailed file links and length of time to hold an inactive user interface open.

SUMMARY

Nimbus Technology takes the security and privacy of customer data very seriously and it is a cornerstone of the Nimbus reputation. There are no "backdoors" for support staff and the facilities are designed to withstand independent audit if necessary.

- Redundantly hosted at paired secure world class data centres.
- All transmission of file data and metadata occurs over encrypted channels (https).
- All user files stored on Nimbus servers are encrypted to each account (AES-128).
- Nimbus websites have been hardened and fire walled against hacker attack.
- Nimbus support staff are not able to view any customer data files.
- Nimbus support staff have no login access to Practice sites or Client portals
- Each Practice site and their Client portal have private unique URL's.
- User files are only accessible by people with valid logins to a valid account URL.
- Self managed unique logins ensure privacy of login details.
- Optional two factor authentication exists for password reset.
- Practice web folders are not browsable or searchable via the web or Management console.

--- 0000 ---