



NoteVault Security Outline

March 2011

1	Overview.....	3
2	Technology.....	3
2.1	Website.....	3
2.2	Customer Database.....	3
2.3	US Based Services Telephony Access.....	3
2.4	Middle East Services Telephony Access.....	3
2.5	Firewalls.....	4
3	NoteVault Service.....	4
3.1	Subscriber Log on Security.....	4
3.2	Time Stamping Of Notes.....	4
3.3	Audio Records.....	5
3.4	Recovery of Deleted Notes.....	5
4	Personnel.....	5
4.1	Independent Transcription Contractors.....	5
4.2	NoteVault.....	5
5	Time Stamp Guarantee Certificate.....	7

1 Overview

The purpose of this document is to provide insight into the approach to security that NoteVault has taken to ensure secure and reliable services for its customers globally.

Some areas of this document are intentionally vague such as in specific locations of equipment and specific safety measures taken. The intent of this document is not to provide any assistance to any potential threat from the Internet, of which there are a few to contend with.

NoteVault relies on 3rd party providers to facilitate the process of capturing voice, transcription, and the housing of information. Their respective security policies are attached as references in the annex for further review by customers should they wish.

2 Technology

2.1 Website

NoteVault is hosted at 1&1 located in the US. Data centers are comprised of steel-reinforced walls, fire protection via the combination of an early detection system + FE-25 system + double-interlock pre-action sprinkler system, backbone routers from two different vendors, redundant cooling systems and redundant UPS systems in addition to diesel generators ensure top-of-the-line security so that servers will continue to operate regardless of external conditions. 1&1 provides 99.9% uptime and 24/7 technical support.

2.2 Customer Database

The customer database is housed with Amazon Web Services. A complete details of security related to Amazon Web Services can be found at <http://aws.amazon.com/security/#overview>.

Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities. It is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year, and sustain the concurrent loss of data in two facilities.

2.3 US Based Services Telephony Access

In the US and most of the world, connectivity (telephone No.s) can be provided by use of whole sale telecoms companies. These telephone numbers are trunked to a SIP based PABX system that NoteVault then receives postings to its web site on. The in call reliability is therefore equivalent to that which operators generally offer for most voice service subscriptions.

2.4 Middle East Services Telephony Access

The Middle East region has two main issues different to the US and the rest of the world.

- a. In most countries SIP or Voice over IP is illegal
- b. Internet access can be problematic.

To overcome these challenges, NoteVault has set up a distributed voicemail architecture that uses mobile trunks to receive a voice mail and then attaches this voicemail to an SMTP service to deliver securely to the NoteVault database for processing. This equipment is housed in a data warehouse that has:

- a. Independent redundant connections to the Internet
- b. Universal Power Supply independent from the grid to provide power indefinitely
- c. Fast cool fire retardant technology

Many large corporate companies house and maintain their equipment in this data warehouse. Access is tightly monitored with 24 X 7 security. No person (including those authorized to enter the facility) is allowed access without being escorted at all times.

2.5 Firewalls

NoteVault uses the following firewall technology:

NoteVault hosting provider 1&1 provides a Cisco based hardware firewall externally to protect from any potential known attacks to our servers before any request are being passed through. It also allows ability to configure custom firewalls specific to our services through a secure control panel.

Software is always up to date and the system is audited periodically to ensure that latest best practices are used to ensure site up time and protection of customer data.

3 NoteVault Service

3.1 Subscriber Log on Security

Each subscriber is provided with a unique log on and encrypted password which can only be changed by:

- The subscriber themselves

Users are required to change default password on first login.

NoteVault customer service is authorized to send out a temporary password to replace a lost password. Users are required to change temporary password on first login

3.2 Time Stamping Of Notes

All notes received by NoteVault are 3rd party time stamped. This time stamp is intrinsic to the integrity of the service when it comes to subsequent discussions

between NoteVault customers and third parties. See Time Stamp Certificate in this document for further information.

3.3 Audio Records

All audio records are transcribed in to the best possible text version of that audio that is achievable by our transcription staff. The audio itself is saved for as long as a customer is a paying customer of NoteVault and if evidence needs to be presented in a dispute process, the audio is the primary reference.

These audio notes can not be tampered with in any way for any purpose save for deleting a note all together.

3.4 Recovery of Deleted Notes

It is possible for NoteVault to recover a note that has been deleted by accident by a subscriber.

4 Personnel

There is a controlled group of personnel who by virtue of their job are an intrinsic part of enabling the NoteVault service. Apart from administrators there is transcription staff who physically transcribe notes from the field. Typically this is facilitated by two organizations.

- Level One - Independent Transcription Contractors (under confidential terms)
- Level Two - NoteVault internal resources.

4.1 Independent Transcription Contractors

Security ensured by:

- The transcribers only have an audio file (no other information about the person leaving the note)
- Voicemails are randomized, so it's extremely rare the same transcriber gets more than one of your voicemails.
- All transcribers have signed agreements to preserve privacy with material penalties for violating it, similar to what is used in the medical industry to transcribe medical records.

4.2 NoteVault

NoteVault has staff who provide Quality Control of the transcription. This is to ensure a high level of quality in the resultant reports. Similar to the approach taken in the medical and legal industry security is assured by:

- Non-Disclosure Agreements
All NoteVault personnel sign non disclosure agreements
- A complete record of which transcriber saw which notes is retained in the system.
- Transcribers are limited to cover a certain region

NOTE  VAULT™
The Ultimate C.Y.A.™

NoteVault. The one power tool you can't be without™.
Commercial in Confidence

- Transcribers are managed daily by Notevault management to ensure quality and security.

5 Time Stamp Guarantee Certificate

This section of the NoteVault Security Outline document serves as the certificate of accuracy of time stamps associated with all notes received by the NoteVault system and as submitted by Notevault subscribers.

The time is taken from GMT and is then adjusted for appropriate time zones for display purposes.

It is not possible for any subscriber to change the time stamp associated with a note previously delivered to NoteVault. The only extent to which a time can be interfered with in a Note is to delete that Note all together.

To avoid confusion, it is not possible for a subscriber, or any party to tamper with a time stamp on a note for any purpose what so ever.