NEXTPOINT

SECURITY & PRIVACY

Ensuring the confidentiality, integrity, and availability of customer data

SECURITY

NEXTPOINT.COM

SECURITY AND PRIVACY AT NEXTPOINT

OVERVIEW

Ensuring the confidentiality, integrity, and availability of customer data is of the utmost importance to Nextpoint. In addition to hosting its applications on Amazon Web Services, the most secure data host available, Nextpoint has a dedicated infrastructure and security officer responsible for ensuring the protection of all client data.

We have no higher priority than the privacy and security of our clients' data. We aim to lead the industry as a trusted repository for client data and are continually seeking to strengthen that position.

.

SECURE

Security risks are assessed on an ongoing basis by Nextpoint's Site Reliability Engineer.

A COMPANY-WIDE COMMITMENT

All new hires undergo background checks before formally starting work as well as security training as part of the Nextpoint onboarding process. Following successful completion of the training, employees sign a confidentiality agreement regarding the protection of client information. Additionally, all employees, regardless of tenure, participate in annual security training.

Security risks are assessed on an ongoing basis by **Nextpoint's Site Reliability Engineer**. These assessments include running a weekly vulnerability scan, reviewing controls each month, and conducting an annual comprehensive IT risk assessment.

THE MOST SECURE DATA HOST AVAILABLE

Security within Nextpoint products are provided on multiple levels: the operating system of the host system; the virtual instance operating system, or guest operating system; a stateful firewall; and signed API calls. Each of these items builds on the capabilities of the others.

Nextpoint products are deployed through **Amazon Web Services**. Amazon Web Services far surpasses even the strictest privacy and security standards, including standards held by the United States Department of Defense. Simply put, there is no more secure and dependable service for storing electronic data.

ACCESS CONTROLS

Data is **encrypted both at rest and in storage**. Data processing takes place on virtual machines explicitly provisioned to serve only one client per lifetime.

Physical access to data centers is strictly controlled both at the perimeter and building ingress points by professional security staff. State-of-the-art video surveillance and intrusion detection systems ensure security.

All employee **data access is documented via a documentation trail**. This trail includes both documentation of the request and the granting of that request by an authorized party. Multi-factor authentication and session timeouts further guard against unauthorized access.

SYSTEM AVAILABILITY AND BACKUP

Nextpoint products hosted by Amazon Web Services are designed to provide **99.999999999% durability of objects** over a given year. Amazon S3 redundantly stores your objects on multiple devices across multiple facilities in an Amazon S3 Region.

Nextpoint is fully prepared for complete data recovery and an immediate return to service following an accident or disaster.

DATA DESTRUCTION

Nextpoint will delete customer data upon request. Nextpoint uses hosting providers that follow hardware protocols to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.

INCIDENT RESPONSE AND BREACH NOTIFICATION

Nextpoint's Site Reliability Engineer reviews firewall notifications and operating system event logs on a daily basis. The officer also monitors access levels to secured technologies (AWS,

BACKUP

Nextpoint products hosted by AWS are designed to provide 99.999999999% duribility of objects over a given year.

the network, the application, etc.) and failed login attempts to the application.

If Nextpoint discovers there may have been an incident in security which has or may have resulted in unauthorized access to Nextpoint protected data, **we notify potentially affected users as soon as it's possible** to do so without compromising any investigation or remediation of the breach.

PRIVACY

Nextpoint takes the overly cautious position of assuming customer data is highly sensitive. In addition to strictly adhering to the GDPR, Nextpoint adheres to numerous other privacy regulations by hosting data with Amazon Web Services, which complies with the strongest regulations in effect worldwide. For more information on Amazon Web Services and privacy regulations compliance, see here. **Read Nextpoint's privacy policy in full.**

Nextpoint takes the overly cautious position of assuming all customer data is highly sensitive.

ABOUT NEXTPOINT

Nextpoint is smart software that automates ediscovery projects for legal teams of every size. The highly secure, cloud-based solution lets your team begin document review in minutes with powerful data analytics tools, a user-friendly interface and collaborative access from anywhere. Innovative trial-prep features will exceed your expectations of what smart ediscovery software can do.

STOP PAYING FOR EDISCOVERY DATA!

Nextpoint gives users **free, unlimited data uploads, processing, hosting, OCR, imaging and productions.** As you face increasing pressure to control costs, Nextpoint empowers users to easily process, analyze, review, produce and present data, affordably and predictably.

Founded as a litigation support company in 2001, Nextpoint introduced the world's first cloud-based litigation software a few years later. Since then, we've continued to innovate and expand to serve law firms, corporations and government agencies of all sizes. In 2013, Nextpoint was awarded U.S. Patent number 8,447,731 for our management of electronic data in the cloud, specific to litigation processes.

Learn more about Nextpoint

Visit: nextpoint.com
Email: hello@nextpoint.com
Call: **1.888.929.NEXT**
Twitter: **@nextpoint**