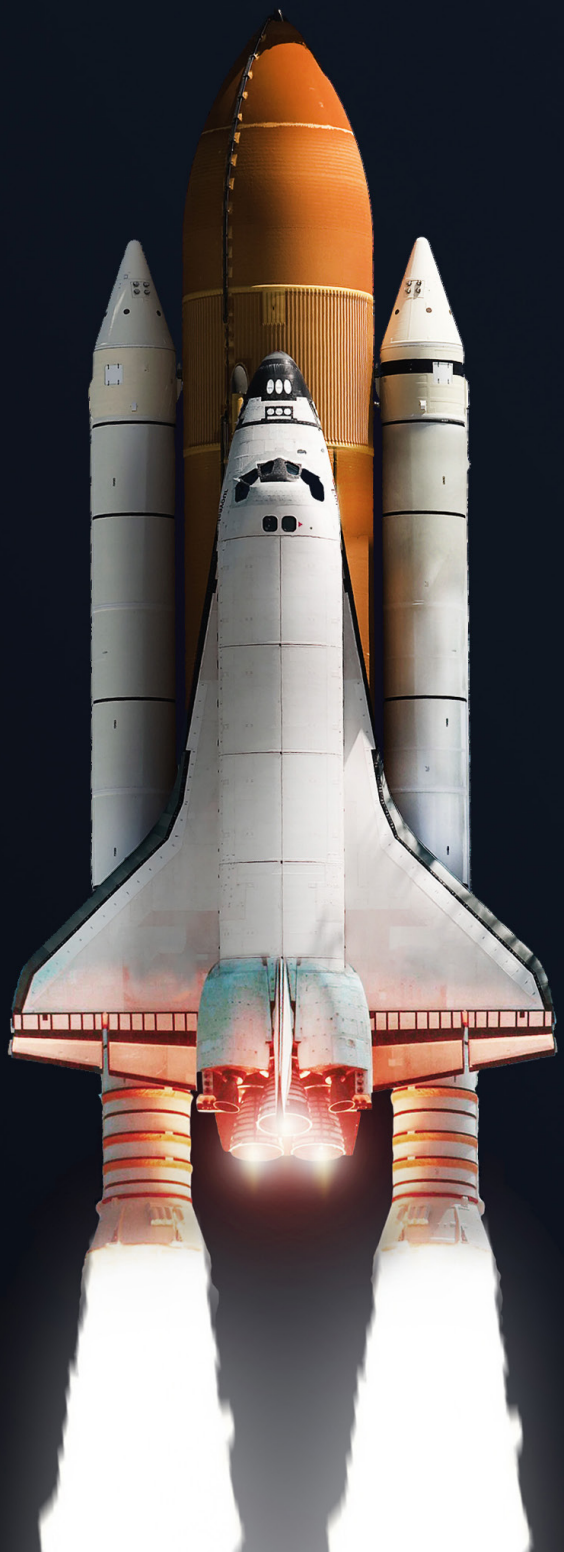
nexoid

Data and Security Policy



Version
2024.1.0.3

Data And Security Policy Statement

In today's digital environment, data has become the lifeblood of businesses, acting as a catalyst for growth, innovation, and informed decision-making. As a B2B SaaS company, Nexoid recognises the crucial role that data plays in our clients' operations. We acknowledge that data is not only precious but also susceptible, perpetually at risk from cyberattacks and security breaches. Hence, we place data protection and security at the heart of our offerings.

The surge in cyberattacks and the mounting expenses linked to data breaches emphasise the necessity of robust security measures. Over the past ten years, the digital sphere has seen a disturbing rise in cybercriminal activities, targeting businesses of all scales and sectors. These attacks have not merely led to monetary losses but have also inflicted lasting harm to brand image and customer confidence. As a result, companies are more alert than ever in protecting their data assets and curtailing potential security threats.

We recognise that the security of your data is paramount. We comprehend the potential repercussions of a security lapse, encompassing financial liabilities, legal consequences, and damage to reputation. Therefore, we've adopted thorough security protocols and best practices to guarantee the highest protection of your invaluable data. Our dedication to data security spans all facets of our operations, from the creation and roll-out of our software solutions to the continued maintenance and support we offer to our clients.

Compliance

We harness the power of AWS (Amazon Web Services) serverless architecture to enhance our data security and operational efficiency. By leveraging serverless computing, we remove the need for us to manage individual servers, reducing risk and allowing us to focus on delivering superior products to our clients. Amazon is the largest web hosting company in the world, a true global tech giant. AWS not only brings vast infrastructure resources to the table but also adheres to numerous compliance standards and certifications. This ensures that our serverless environment is underpinned by Amazon's world-class security and reliability measures. By aligning with AWS, Nexoid offers its clients a robust, military-grade, scalable, and secure data handling architecture. Amazon AWS is compliant with the following standards.

ISO 27001: The International Organization for Standardization's ISO 27001 is a globally recognised standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive company information so that it remains secure, encompassing people, processes, and IT systems. Nexoid follows the best practices set out by ISO 27001 to ensure a resilient and robust security infrastructure.

SOC 2: Service Organization Control (SOC) 2 is a standard designed for technology and cloud computing entities. It evaluates a company's information systems in terms of their security, availability, processing integrity, confidentiality, and privacy. At Nexoid, we've structured our systems and operations to meet and often exceed the expectations laid out by SOC 2.

GDPR: The General Data Protection Regulation (GDPR) is a regulation in EU law that deals with data protection and privacy. It's designed to ensure that individuals have control over their personal data and harmonises the regulatory environment for international business. While Nexoid operates outside the EU, we abide by GDPR principles, demonstrating our commitment to safeguarding client data on a global scale.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. regulation that establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information. Though its primary application is in the healthcare sector, its principles underscore the gravity of data

protection. Nexoid integrates the best practices from HIPAA into our own procedures to ensure that sensitive data, health-related or otherwise, is treated with the utmost respect and care.

Employee Training and Awareness

We believe that the strongest security systems are only as robust as the people behind them. Recognising this, we are deeply committed to continuously educating our employees about the evolving landscape of IT security. Regular training sessions are held, ensuring that every member of our team remains updated on the latest threats and best practices in cybersecurity. These sessions are more than mere lectures; they are comprehensive programmes that test our employees' knowledge, ensuring that theoretical understanding translates into practical preparedness.

Additionally, our dedication to security doesn't stop at training alone. We frequently undertake reviews of the latest best practices in the realm of IT security. This proactive approach ensures that Nexoid not only meets the current industry standards but often exceeds them. By combining consistent training with a culture of continuous improvement, we ensure that our team is always equipped to handle the challenges of today's digital landscape, fortifying our commitment to safeguarding our clients' data.

Physical Security

Amazon Web Services (AWS) is globally recognised for its unparalleled digital prowess, but equally commendable are its stringent physical security standards. The foundations of these data centres are akin to modern fortresses, where both infrastructural elements and the vital data within are safeguarded with military precision.

Entry into AWS data centres is a privilege afforded to a select few. Each individual vying for access undergoes a rigorous vetting process, ensuring only those with impeccable credentials are granted admission. This meticulous scrutiny aligns with the highest standards, including those that are synonymous with military requirements.

The sanctity of data is of paramount importance to AWS. Consequently, its protocols surrounding data disposal and equipment replacement are inflexible and exacting. When data is marked for deletion, AWS employs procedures that ensure its complete and irreversible destruction. Similarly, the replacement of drives and other hardware components adheres to tight procedures that guarantee the permanent eradication of old data. This ensures that no vestige of data lingers beyond its intended lifecycle, preserving the trust clients place in AWS.

Nexoid's partnership with AWS is built on trust and respect for these robust security paradigms. So much so, that even our personnel do not have access to these data centres. The secrecy extends to such an extent that our team remains uninformed of the exact physical locations of these facilities. This reflects AWS's commitment to an elevated security standard, where the specifics of their operations remain undisclosed, even to strategic partners.

The combination of AWS's rigorous physical security, which is on par with military-grade standards, and their robust digital defences, assures Nexoid's clientele that their data is housed in one of the most secure environments conceivable.

Cyber Attacks and Threats

In today's digital age, the threat landscape is continuously evolving, presenting new challenges that organisations must tackle to safeguard their data and systems. At Nexoid, we recognise the paramount importance of robust cybersecurity measures, and to this end, we have fortified our systems with state-of-the-art solutions.

Central to our defence strategy is the integration with AWS CloudFront, a leading content distribution system. This not only ensures efficient content delivery but, more critically, acts as a formidable shield against certain types of cyber threats. Specifically, AWS CloudFront offers protection against Distributed Denial of Service (DoS) attacks, which aim to overwhelm and incapacitate targeted systems by flooding them with traffic. By distributing incoming traffic across its vast global network, CloudFront effectively diffuses the potency of such attacks, ensuring our services remain uninterrupted.

In addition to its defence against DoS attacks, CloudFront significantly minimises the risk associated with direct server attacks. Rather than accessing Nexoid's individual servers, potential attackers would need to penetrate the robust defences of CloudFront first, a task that is daunting to even the most sophisticated adversaries.

One of the most commendable features of CloudFront is its dynamic firewall capabilities. This superlative firewall acts as a vigilant gatekeeper, strictly regulating what can and cannot access our systems. By controlling port access, masking the visibility of IP addresses of machines, and filtering malicious traffic, it ensures that only legitimate requests reach our infrastructure. Such stringent measures drastically reduce the potential attack vectors, providing an additional layer of security.

In conclusion, while the cyber realm is fraught with potential threats, Nexoid, through its strategic partnership with AWS and the deployment of CloudFront, ensures that our systems remain resilient and secure. Our clients can have confidence in the knowledge that their data and interactions with our platform are protected by some of the most advanced cybersecurity measures available.

Access Control, Auditing and Monitoring

Our approach to security is both multi-faceted and unwavering. By instituting rigorous access control, robust auditing, and vigilant monitoring systems, we ensure the sanctity of our client's data at every juncture.

It's essential to underline that Nexoid staff do not inherently have access to any client's account. Instead, any access we gain is strictly on the client's terms; they must grant it explicitly. Although we require this access to deliver optimal support, the power to grant or revoke it remains solely with our clients, underscoring our commitment to client autonomy.

Integral to our monitoring system is the vigilant logging of a wide array of activities. Each sign-in attempt, be it successful or otherwise, is recorded, capturing both the IP address and computer ID for heightened security. Furthermore, any activity within an account, whether it's reading, editing, creating, deleting, or searching records, is scrupulously audited. In instances where IP addresses or user accounts raise red flags, our system proactively blocks them, ensuring potential threats are swiftly neutralised.

Our commitment to safeguarding user credentials is unwavering. Passwords are not stored in plain text. Instead, they undergo encryption using a one-way SHA-512 hash, bolstering their security. But our innovation doesn't stop there. The hashing algorithm we employ varies for each client and user account. This unique differentiation renders hash attacks virtually unfeasible, as attackers would be forced into the laborious process of brute-forcing each account individually, an endeavour that is both time-intensive and highly unproductive.

Adding another layer to our security matrix, we offer two-factor authentication through Single Sign-On (SSO), facilitated by synchronisation with platforms like AD Azure or Google Workspace. This synergy ensures that if a user's access is terminated on these platforms, their Nexoid account is instantaneously blocked, reflecting a seamless security echo.

Lastly, in emergency scenarios, we provide a failsafe with our "panic button" feature. A single activation terminates all live sessions and locks the system, restricting access solely to administrators. This immediate response mechanism ensures swift containment of any potential breaches.

Data Storage Standards

At the forefront of data storage and security, we offer our clients unparalleled options that cater directly to their specific needs. Central to our approach is the regionalisation of all client data. This system not only ensures that every piece of information is backed up and stored in a redundant manner but also allows it to be housed within a singular jurisdiction region, as chosen by the client. This unique offering establishes Nexoid as one of the few companies providing compliance at a country-specific level, assuring our clients of unwavering data sovereignty and adherence to localised regulations.

Every jurisdictional region in our infrastructure has a minimum of three, often extending to four, expansive data centres. Client data is securely stored in at least three of these centres, ensuring redundancy and resilience. The sophistication of our system is evident in the seamless and automatic replication of data across these centres, guaranteeing real-time data availability. Further reinforcing our commitment to data security, all communications within Nexoid's architecture and between our platform and clients are encrypted using RSA 2048 M01 SSL certificates, supplied by the industry leader, Amazon AWS.

Customer empowerment is a core tenet of our service. Clients have granular control over security within their accounts, having the authority to bestow both object and record-level permissions to users. A distinct feature of Nexoid is our system's capability to permit multiple ownerships for a singular data record, a rarity in the industry. Moreover, Nexoid enforces rigorous data auditing protocols. Every action, be it reading, writing, updating, searching, or deleting, is meticulously logged, noting both the user involved and the corresponding IP address. By default, data is encrypted at rest, ensuring an added layer of security. Internally, our access to the AWS cloud is stringently restricted, with account permissions meticulously calibrated to remain minimal, aligned only with the specific tasks at hand.

Data Collection

Large scale data analysis is the key to designing good products and services. We value the insights that our customer data offers, we equally uphold the principle of client privacy and the ethical use of such data.

When we collect data, the primary objective is to enhance system performance and drive continuous improvement. To ensure client confidentiality, all data that Nexoid gathers is anonymised. This process strips away any identifying attributes, ensuring the information cannot be traced back to any specific individual or entity. While this anonymised data aids us in refining our systems and services, it's crucial to note that Nexoid maintains a strict policy against external data sharing. We never publish or disclose this data to any third-party entities, guaranteeing our clients' privacy.

On occasions where insights are distilled from the amassed data, they are presented in the form of meta-reports. These reports provide high-level information, offering broad overviews without delving into specifics. The intention behind such reporting is purely analytical, aimed at understanding trends and patterns rather than individual actions or attributes.

Clients at Nexoid are given the agency and choice when it comes to their data. We understand and respect the prerogative of our clients to opt out of our data collection process. However, it's worth noting that by participating in our data analysis, clients stand to benefit in more ways than one. A significant advantage of this analysis is our capability to identify potential misuse or irregular activities within the client's account. This not only ensures that their data remains protected but also aids in safeguarding the overall integrity and security of their account. By being a part of our analysis system, clients bolster their own security framework, ensuring that their data and accounts are shielded from both external and internal threats.

Disaster Recovery

Our commitment to data security and availability is evident in our rigorous backup protocols. Every 24 hours, Nexoid carries out a full backup of all data, capturing every detail and ensuring nothing is overlooked. This complements the formidable infrastructure provided by Amazon Web Services (AWS), which performs its own comprehensive backups every hour. The synergy between Nexoid's internal procedures and AWS's expansive resources guarantees that our clients' data is constantly safeguarded, offering multiple layers of redundancy.

Recognising the importance of flexibility and control, we also empower our clients with the ability to initiate their own backups. They can choose between creating full account backups or focusing on specific segments of their data, providing them with a tailored safety net. Additionally, in the event of any data-related issues, clients have the autonomy to restore their accounts fully or partially, depending on their unique requirements. This combination of automated and user-driven backup and recovery options ensures that Nexoid's clients always have immediate access to their data, regardless of any challenges that may arise.

Incident Response and Communication

In the realm of cybersecurity, proactive monitoring and swift incident response are indispensable to ensuring optimal system integrity. We have developed advanced systems specifically designed to detect and respond to suspicious behaviours at the earliest possible juncture. These systems continuously scan our platform, searching for anomalies that might indicate a security breach or system compromise. Upon detection of any such irregularity, our dedicated incident response team is immediately alerted and springs into action, launching a comprehensive investigation to understand the nature and extent of the threat.

However, our responsibility doesn't end with mere detection and response. Recognising the potential impact on our clients, we've integrated an emergency shutdown system that can be activated in particularly critical situations. This ensures that, in the face of significant threats, we can swiftly contain and manage the situation, minimising potential damage.

Transparency is a cornerstone of our operational philosophy. Should any breach or outage occur, our commitment is to keep our clients informed from the outset. We believe that our clients have a right to be aware of any situation that may affect their data or the functionality of our services. Therefore, as soon as we identify an incident, affected clients are notified, ensuring they're not left in the dark and can take any necessary actions on their end.

In line with our transparency ethos, we also offer live status updates accessible to everyone via our public website. This provides real-time information about the health of our platform, any ongoing incidents, and the measures we're taking to address them. Such public reporting not only reinforces our accountability but also underscores our unwavering dedication to ensuring our clients remain informed and empowered at all times.