Novi AMS Security & Compliance Overview

Last Updated: January 20, 2025

At Novi, we understand that members are the lifeblood of your organization, and your membership database is the key to keeping them engaged. That's why the security of your membership data is critically important. We have developed our security framework using best practices for the SaaS industry, with four key objectives guiding our approach:

- **Customer Trust and Protection** – We strive to deliver superior products and services while protecting the privacy and confidentiality of your data.
- **Availability and Continuity of Service** – Our focus is on ensuring service availability and minimizing risks to service continuity.
- **Information and Service Integrity** – We take measures to protect your information from being corrupted or altered inappropriately.
- **Compliance with Standards** – We aim to comply with or exceed industry standard best practices.

To safeguard the data entrusted to us, Novi takes a multi-layered approach to security. We implement a combination of administrative, technical, and physical controls across our entire organization. Below is an overview of some of the key security measures we are frequently asked about.

Infrastructure

Cloud Technology
Our system is hosted on Microsoft Azure, a cutting-edge cloud infrastructure. By partnering with Microsoft, we leverage a global team of experts to help ensure your data is protected at the highest level.

Microsoft Azure's status is available here. Information on Microsoft's SOC 2 Type 2 report is available here.

Network Boundary

Novi's infrastructure employs multiple layers of filtering and inspection for all connections through our web application firewall (WAF), logical firewalls, and security groups. Network access control lists are used to block unauthorized access to our internal systems and resources. Firewalls are set by default to reject any network connections unless they have been explicitly approved, with traffic monitoring in place to detect any unusual activity. Changes to our network and perimeter systems are closely tracked and managed through standardized change control procedures. Our internal team and an external consultant regularly review firewall rules to ensure only essential connections are permitted.

Highly Automated and Scalable Infrastructure

The product infrastructure operates within a highly automated environment designed to adjust its capacity based on demand dynamically. This scalability ensures that resources are provisioned and de-provisioned as needed, optimizing performance and cost-efficiency. Automated monitoring tools continually assess system requirements, allowing the infrastructure to expand seamlessly when traffic or data processing needs increase and scale down when demand decreases.

Comprehensive Logging and Monitoring
We maintain comprehensive logging systems to capture critical data across various aspects of our infrastructure and applications. Our logging framework includes:

- **Error Logging**: Captures and records system errors, application faults, and exceptions to ensure rapid diagnosis and resolution.
- **Action Logging**: Tracks user actions and administrative activities to maintain accountability and support troubleshooting efforts.
- **Network Activity Logging**: Monitors network traffic, access requests, and potential threats to detect unauthorized access or unusual patterns.
- **Server Activity Logging**: Records server performance, resource usage, and operational health to optimize efficiency and detect any issues.
- **Performance and Uptime Monitoring:** We continuously track the performance and availability of both the application and our customers' individual websites. This includes real-time alerts and historical uptime records for ongoing quality assurance. Our status page shows uptime performance for the last 90 days.

These logging capabilities provide valuable insights into system performance, help identify potential issues early, and support both security and operational excellence. Logs are securely stored and regularly reviewed to ensure the ongoing health of our infrastructure and customer environments.

Application Security

Microsoft Front Door - Caching for Enhanced Performance and Protection
Your Novi subscription includes a subscription to Microsoft Front Door, which enhances your website's performance and security. The system utilizes intelligent caching mechanisms to optimize performance and safeguard against threats like bot attacks and denial-of-service (DoS) attempts. By caching frequently accessed pages and resources, we reduce the load on our servers, ensuring faster response times for legitimate users.

Caching also protects against traffic surges or malicious attacks. By serving cached content instead of overloading the application or backend systems, it limits the impact of excessive requests. This approach helps mitigate the effects of bot traffic and DoS attacks while maintaining the availability and performance of both the application and our customers' websites.

Malware Scanning with Microsoft Defender for Cloud
Novi AMS integrates advanced malware scanning powered by Microsoft Defender for Cloud to provide real-time protection for files stored within your system. Leveraging Microsoft's intelligent threat detection, we continuously monitor for potential malware threats. This proactive approach helps defend against malicious software from infiltrating your environment, offering quicker response capabilities to any suspicious activity.

Content Security Policy (CSP) Headers
To protect against XSS attacks, we employ CSP headers that control resources the browser is allowed to load, reducing the risk of malicious scripts executing on our applications.

Parameterized Queries
To prevent SQL Injection, we use parameterized queries, which ensure that database queries are safely constructed and executed and that user inputs are appropriately handled.

Spam Prevention
Every Novi AMS subscription includes multiple layers of spam protection to ensure secure and reliable form submissions. Forms submitted through the Novi platform require reCAPTCHA verification, which helps prevent spam and bot activity by verifying that a human is initiating the action.

To further enhance protection, Novi AMS monitors emails for spam keywords and maintains a global list of profanity and other terms that may indicate spam. Admins can also add custom words or phrases to this block list, tailoring it to their specific needs. Messages containing a combination of blocked words are automatically prevented from being delivered, providing an additional safeguard against unwanted or malicious content.

Regular Vulnerability Scanning and Patching
Our systems undergo continuous vulnerability scanning to identify potential risks promptly. We also maintain a strict patching schedule to ensure our applications are equipped with the latest security protections.

Structured Code Deployment Schedule
At Novi AMS, we follow a structured deployment schedule with updates to our application released roughly every two weeks. This schedule helps us mitigate risk while ensuring timely updates and improvements to the platform. Our development team works in two-week cycles, called sprints, during which we prioritize, develop, and test new features or bug fixes. After a sprint concludes, we conduct thorough QA testing during a stabilization period before deploying the new code the following week. Testing is both automatic and manual in nature.

Why do we stick to a two-week cadence? It ensures that we're never far from addressing potential issues and allows us to release manageable, incremental changes. This approach reduces the risk of large-scale updates, which can introduce more complications. It also helps to ensure that our customers have plenty of time to adjust to smaller, incremental changes instead of large, jarring ones.

We maintain a high threshold for releasing updates outside of our regular schedule. An unscheduled or "out-of-band" release only occurs if a critical issue severely impacts business operations or causes monetary disruption. These events are rare, as deploying code involves some risk, even with extensive automation and testing. Our priority is to ensure that every update is fully tested and stable, avoiding half-completed changes from being deployed.

Additionally, our deployment process is designed to ensure zero downtime. We release updates to a separate server and swap it instantaneously with the active server, allowing for seamless transitions without disrupting service.

For larger features, we often employ a beta process, inviting customers to participate in testing and providing valuable feedback on usability. This collaborative approach helps us refine features before full deployment, ensuring they meet customer needs and expectations.

Outside Review
At Novi AMS, we employ a multi-layered approach to vulnerability management. We use a combination of industry-recognized tools and threat feeds to ensure our technology stack is comprehensively protected. Our vulnerability scans are configured to run daily, utilizing adaptive scanning techniques for asset discovery and the latest detection signatures to identify potential risks.

In addition to our internal processes, we engage third-party experts to perform annual penetration tests on our applications and infrastructure. These assessments help us uncover vulnerabilities that may pose security-related risks. Findings from these reviews are carefully evaluated, with mitigations prioritized to ensure that any identified risks are swiftly addressed.

As required to be listed in the QuickBooks App Store, Novi undergoes a voluntary security review led by Intuit and QuickBooks each year. Their team rigorously tests our systems for vulnerabilities, ensuring we meet their stringent standards for financial data security.

Data Protection

Data Classification
Novi AMS allows customers to define the types of information they collect and store within our platform. In line with the Novi AMS Terms of Service and Acceptable Use Policy, our customers must ensure that the data they capture is appropriate and relevant for supporting their marketing, sales, services, content management, and operational processes.

It is important to note that Novi AMS products are not intended to collect or store sensitive information, as outlined in our Terms of Service. This includes, but is not limited to, credit or debit card numbers, financial account details, Social Security numbers, passport numbers, or any financial or health-related information. Customers should avoid collecting such sensitive data to maintain compliance and ensure proper data security.

Tenant Separation
Novi AMS operates as a highly scalable, multi-tenant SaaS solution. Customer data is logically separated using unique portal IDs, ensuring that each customer's data and associated objects remain securely isolated and associated only with their specific account.

Our platform is designed with strict authorization rules that are embedded into the architecture and continuously validated to ensure secure access and data integrity. Additionally, we maintain logs that

capture critical information, including application authentication events, associated changes, application availability, and user page views, providing transparency and accountability for system activity.

SSL Certificates for Customer Websites
At Novi AMS, we provide **SSL certificates** for all our customers' websites to ensure secure, encrypted communication between the site and its visitors. SSL (Secure Sockets Layer) certificates are essential for protecting sensitive information, such as login credentials and personal data, by encrypting data exchanged over the internet.

With SSL certificates in place, your website will display the trusted **HTTPS** protocol, giving your members confidence that their interactions with your site are secure. This built-in security measure helps protect your users' data and supports compliance with industry standards for online security.

Encryption
At Novi AMS, we prioritize the security of sensitive interactions by ensuring all data in transit is encrypted using Transport Layer Security (TLS) version 1.2 or 1.3, with 2,048-bit keys or stronger. This includes API calls, authenticated sessions, and other sensitive communications. For customers hosting their websites on the HubSpot platform, TLS is also the default protocol for secure data transmission.

Novi AMS utilizes Microsoft SQL Server's encryption technologies to protect data at rest and ensure that stored information remains encrypted. Additionally, user passwords are hashed immediately before being saved in our database, following industry best practices to safeguard credentials.

Secure File Exports
Data export files are transmitted through secure channels to protect the integrity and confidentiality of the information. Each file is secured using a Globally Unique Identifier (GUID), which provides an additional layer of protection by making it accessible only through its unique, secure link.

Furthermore, access to exported files is restricted to logged-in users with the appropriate access level. This ensures that only authorized users can view or download sensitive data, further enhancing the security of exported information.

PCI Compliance
Novi AMS integrates with QuickBooks Payments and Stripe to facilitate the secure processing of credit card payments for your organization. All connections between Novi AMS and these payment providers are architected in a PCI-compliant manner, ensuring that the highest security standards are met throughout the transaction process.

While Novi AMS provides the platform for initiating and managing transactions, your members' credit card data is never stored on our servers. This design ensures that the payment processors handle sensitive payment information directly, keeping your organization in line with Payment Card Industry Data Security Standard (PCI DSS) requirements and safeguarding your members' financial data.

It is important to remember that while Novi handles certain aspects of PCI compliance, your organization is still responsible for adhering to PCI requirements related to your business practices. These include securing your network environment, managing user access, and maintaining proper documentation and

training. For additional information about PCI compliance, visit the PCI Security Standards Council (PCI SSC) or contact your payment processor.

Data Backup and Disaster Recovery

Backups
We provide a comprehensive backup system to ensure that your member data is securely stored and easily recoverable in the event of an issue. Our system utilizes point-in-time backup capabilities, giving us the ability to restore your data with flexibility. This means that if data is lost or corrupted, we can help recover what was missing.

To further enhance data security, our backups follow a globally redundant model. This ensures that your data is not stored in just one location. If a data center on the East Coast were to experience an outage, for example, another copy of your data would be safely stored on the West Coast, ensuring that it can be recovered.

Our backup schedule is both comprehensive and systematic.

- Daily backups are stored in the local region for quick access.
- Additionally, backups are periodically copied to a separate Azure data center, allowing for recovery in the event of a primary data center failure.
- We retain seven days' worth of backups for any database, ensuring easy restoration if needed.
- Microsoft maintains these backups for a rolling 35-day period. We also retain monthly backups for 6 months and yearly backups for 2 years to provide additional long-term protection.

All of these backup systems are included with your Novi AMS subscription. Regular monitoring and alerting systems detect replication failures.

No Physical Backups
We utilize public cloud services for hosting, backups, and recovery operations, eliminating the need for physical infrastructure or storage media. All data is securely stored and managed in the cloud, avoiding traditional physical backups such as hard drives or tapes.

We also do not rely on physical media like paper or tape for any part of our product delivery to customers. Our entirely cloud-based approach ensures that data is efficiently stored and protected without the need for physical storage solutions.

Customer Data Backup Restoration
Novi AMS manages all disaster recovery and resiliency operations, ensuring that customers do not need to manage failover events themselves. Customers do not have direct access to the product infrastructure that would allow them to initiate such actions; instead, our engineering team oversees all recovery processes to maintain system stability and security.

For critical data, such as member records, groups, custom fields, static website content, event listings, and Ecommerce products, Novi AMS implements a soft delete feature. This means that when data is deleted, it can be restored by an admin user with the appropriate access permissions, offering an extra layer of protection against accidental deletions.

Audit Log
Novi AMS provides admin users with access to a comprehensive audit log that tracks key details for every change made within the system. This audit log ensures transparency and accountability by capturing the following information for each modification:

- Date & time of the change
- The user responsible for the change
- Type of user making the change (e.g., admin, member, background process)
- Initial value before the change
- New value after the change

This detailed logging allows admins to monitor system activity and track data updates, ensuring a secure and well-managed environment.

Access Control

Role-Based Access Control (RBAC)
Novi AMS offers flexible access control, allowing administrators to assign users varying levels of access—ranging from full admin rights to limited or page editor roles. This ensures that users can only access the areas they need, protecting sensitive data while maintaining operational efficiency.

Multifactor Authentication
Novi AMS highly recommends enabling Multifactor Authentication (MFA) for all admin users to add an extra layer of security. MFA requires users to verify their identity through two forms of authentication, significantly reducing the risk of unauthorized access.

Users can choose between text message verification or authenticator applications to configure their MFA, allowing flexibility based on individual preferences.

MFA is optional for end users and members, giving them the choice and responsibility to secure their own data.

Password Requirements
We encourage the use of strong, conservative passwords to ensure optimal security. However, all passwords must meet the following minimum requirements:

- At least 8 characters in length
- At least 1 uppercase letter
- At least 1 number
- At least 1 special character

User Account Email Verification

To help prevent fraudulent accounts from being created, Novi requires new users to verify their email addresses. If an email doesn't match an approved domain in your database, the account will be flagged for review, giving you control over whether to accept or deactivate it.

API Keys
Novi's API is a powerful tool that allows your association management system (AMS) data to sync with unlimited third-party tools. To ensure the safety of your data while using the API, API keys in Novi are Base64 encoded strings, which adds an extra layer of security during data exchange.

Each API key can be configured with specific access limitations to control the scope of data that is shared. These restrictions can include:

- Access to specific areas, such as event data, member information, Ecommerce products, website content, blog content, and publicly accessible files like images.
- Limiting access to a segment of member records, which can be defined using a Novi Group to control which members' data is shared.
- Restricting the API key to specific member fields or custom fields ensures that only the necessary information is shared with third parties.

User Activity
Novi AMS includes a comprehensive audit log feature that tracks nearly all changes made within the system, allowing administrators to monitor user activity effectively. This tool captures critical information such as:

- Who made the change
- When the change occurred
- What specific data was altered, including both the original and updated values

Admins can easily access the audit log via the gear icon in the admin interface or through specific sections such as member profiles, events, or transactions. Filters are also available, allowing users to narrow down the audit log by criteria such as the user, component, or date, making it easier to investigate specific changes or actions.

Additionally, the audit log can be exported or shared as needed, providing full visibility into user activities and helping ensure accountability across the platform.

Novi AMS Employee Access
Novi AMS utilizes a Role-Based Access Control (RBAC) model to manage team member access. This ensures that each team member only has access to the systems and data necessary for their role. Access to internal systems and production infrastructure is further secured with phishing-resistant Multi-factor Authentication (MFA) to protect against unauthorized entry.

Access to Novi's internal data stores and production infrastructure is strictly controlled. Day-to-day access is primarily restricted to the Engineering team, ensuring that only essential personnel interact with critical systems, minimizing potential exposure.

In certain cases, customer experience and engineering teams may access individual customer websites to provide support, troubleshoot issues, or implement product enhancements. All access is governed by Novi's Terms of Service, ensuring transparency and security in every interaction.

Corporate Security & Policies

Employee Background Checks
Formal employment offers require all prospective employees to undergo a comprehensive background check conducted by a third-party service. This check includes verification of employment history, educational qualifications, and a criminal background review.

Internal Policies and Procedures
At Novi AMS, all employees participate in a thorough onboarding process upon hire. During this process, they must read and acknowledge the company's key policies. This process ensures that employees are aligned with company standards regarding security and compliance from day one.

To foster a unified approach to data protection, Novi AMS has established several documented policies and procedures. The foundation of these guidelines is our Written Information Security Policy (WISP), which covers essential topics such as proper data management, privacy protocols, and consequences for failing to adhere to policies.

These policies are reviewed on an annual basis to keep them aligned with current best practices and regulatory requirements. All policies are stored in the company's internal knowledge base, and any that require acknowledgment are integrated into the mandatory annual training to ensure all employees stay up to date.

Confidentiality Agreements
Novi AMS requires employees and independent contractors to execute a confidentiality agreement that requires them to follow policies on the protection of customer data.

Security Awareness Training
All Novi AMS employees are required to complete security awareness training within their first 30 days of employment and participate in ongoing quarterly training to maintain a high level of security awareness. This includes general security education, specialized phishing awareness training, and simulations conducted in partnership with a third-party security firm. These simulations help reinforce employees' ability to identify and respond to phishing threats.

Additionally, security is a key focus within the Novi engineering team. Security topics are regularly addressed during sprint planning and sprint retrospective sessions, ensuring that security considerations are integrated into the development process from the start.

Privacy

Safeguarding our customers' data is at the heart of Novi AMS's mission. We are committed to protecting your personal information and ensuring it remains secure, as our Privacy Policy outlines. We take pride in maintaining high standards of data protection.

The security protocols we've implemented and additional layers of protection ensure that your data remains confidential and unchanged. Our comprehensive privacy program is designed to meet regulatory requirements while also addressing the specific needs of our customers and their contacts. Through these efforts, we work to maintain the integrity and privacy of your data at all times.

Members Only Content
With Novi AMS, you can easily lock down content on your website, making it accessible only to members or specific subgroups, such as your board of directors. This allows you to securely share important resources, documents, or communications with the appropriate audience while ensuring that sensitive information remains private and protected from unauthorized access.

Sensitive Data
Novi AMS is not designed to process or store electronic Protected Health Information (ePHI) and does not comply with HIPAA or HITRUST certification standards. For more information about restricted data types, please refer to our Terms of Service, which outline the types of data that are prohibited from being stored or processed in our system.

Data Retention
Customer data is retained for the duration of your active status with Novi AMS. The platform provides tools for data deletion or data export, as outlined in the 'Deletion or Return of Personal Data' section of our Data Processing Agreement (DPA). For more information on how to export your content and data, refer to this article.

For former customers, data is removed from live databases upon written request or after a predefined period following the termination of customer agreements. However, data stored in backups, snapshots, and replicas is not actively deleted but naturally phases out as part of the data lifecycle.

To meet security, compliance, and system performance requirements, Novi AMS retains certain data, such as logs and metadata, even after data removal requests.

Currently, customers do not have the ability to define custom data retention policies within Novi AMS.

Data Breach Notification
In the event of a Personal Data Breach, Novi AMS is committed to promptly notifying customers without undue delay once we become aware of the breach. We will provide timely updates and relevant information as it becomes available or as requested by the customer.

Our detailed responsibilities regarding data breaches are further outlined in our Data Processing Agreement (DPA), ensuring transparency and adherence to best practices in handling such incidents.

Data Privacy Compliance

We recognize that our customers may face myriad of data privacy law compliance requirements. That is why the Novi platform includes several features designed to help customers meet their data privacy compliance requirements. For example, Novi allows users to anonymize records directly within the platform in response to data subject requests. For more information on using these features, as well as Novi's approach to data privacy more generally, please refer to this help article and our Data Privacy page.

It's important to note that while Novi's features can support your data privacy compliance efforts, using Novi alone does not make you compliant with the law. We strongly recommend seeking legal counsel to understand any additional responsibilities or actions that may be required for your organization.

Accessibility

It is important to Novi that its platform and features are accessible to our customers and their members.

Our Commitment

Our team is dedicated to ensuring our customers' websites align with the most up-to-date Web Content Accessibility Guidelines (WCAG) AA standards. The WCAG AA Standards are an internationally recognized set of guidelines that help digital platforms provide accessible services to those with hearing, visual, or other limitations. Although the WCAG AA standards are not a legal standard that guarantees immunity from lawsuits, they represent a best practice for accessibility that aligns with our values and goals.

Achieving digital accessibility is not a static exercise—it's an ongoing, iterative process. Novi's goal is to create websites for its customers that align with WCAG AA standards, and it continuously updates its system to meet these benchmarks. However, achieving accessibility is a shared responsibility.

Customer Responsibility

As a customer, you have full control over the content on your website, which means your organization plays an essential role in ensuring that content remains accessible. While Novi can provide guidance on certain technical aspects of accessibility, we cannot guarantee your website is fully accessible as the law requires.

Independent Accessibility Audits

Our technology is regularly audited by a third party called Access Design Studios. Their team, which includes individuals with firsthand experience with disabilities, uses both technology and lived experience to provide comprehensive accessibility insights. If you utilize Access Design Studios to audit your website, and there are recommendations made to the Novi AMS platform, Novi will incorporate those changes into its upcoming product improvements as part of your partnership with Novi. If recommendations are made for your website content and other embedded, those are the responsibility of the customer.

Important Note About this Document

At Novi AMS, we prioritize transparency in how we deliver solutions to our customers. This document reflects that commitment, providing clear and open information about our practices and protections. However, it is important to note that the content within this document, including any related communications, is for informational purposes only. It does not create any binding or contractual obligations, nor does it alter or modify any existing agreements between Novi AMS and its customers.

As we continuously enhance our security measures and practices, the details provided here may change and improve over time.