novacore

Security and Compliance Framework

Ensuring the Integrity and Confidentiality of Our Digital Ecosystem

www.novacore.ai

Summary

In an era where digital innovation is paramount, Novacore AI stands at the forefront of delivering AI and vision model-based document verification solutions to businesses worldwide. At the core of our mission lies an unwavering commitment to security and compliance, ensuring that our clients' data remains protected against evolving threats and in full alignment with global standards.

This document outlines the comprehensive security and compliance framework that underpins our operations at Novacore AI. Recognizing the critical importance of safeguarding our infrastructure and data, we have instituted a robust security governance model, reinforced by leading-edge technologies and practices. Our approach is designed not only to meet but to exceed industry standards, ensuring that we remain a trusted partner to our clients.

Who We Are

Founded with the vision to revolutionize how businesses verify, validate, and extract data from their documents using artificial intelligence, Novacore AI has rapidly emerged as a pioneer in the B2B technology sector. Our platform enables businesses to seamlessly validate documents through advanced AI and vision models, facilitating improved accuracy, efficiency, and reliability in automating human-centric document related tasks. At Novacore AI, innovation is at our core, driving us to continually evolve our solutions to meet and anticipate the needs of a dynamic marketplace.

Commitment to Security

In today's digital landscape, where the threat landscape is constantly evolving, the significance of robust security measures cannot be overstated. At Novacore AI, we recognize that our technology not only serves to enhance business operations but also plays a crucial role in safeguarding sensitive information. Our security framework is built on a foundation of trust, reliability, and unwavering adherence to global security standards.

OBJECTIVES OF THIS DOCUMENT

1

TO INFORM

We aim to provide our clients, partners, and stakeholders with a transparent overview of the security measures and compliance practices that safeguard our operations and their data.

2

TO ASSURE

By detailing our comprehensive security framework, we seek to reassure all parties of our capability and commitment to protecting the digital assets under our care.

Governance Framework

Our security governance framework is designed to ensure that security considerations are integral to our decision-making processes and operational practices. The framework is overseen by a dedicated Security Governance Board, This board is responsible for:

Establishing and reviewing security policies and standards to align with best practices and regulatory requirements.

01

Overseeing the implementation of security strategies and ensuring their integration into our operational processes.

02

Facilitating cross-departmental collaboration to address security challenges and enhance our security posture.

03

Regularly reviewing and updating our security and compliance programs in response to evolving threats and regulatory changes.

04

Ongoing Compliance with Standards and Regulations

Novacore AI rigorously tries to align itself to internationally recognized security standards and regulatory frameworks to ensure that our practices not only meet but exceed the requirements set forth by these bodies. Our compliance program encompasses the following key standards internally:

- General Data Protection Regulation (GDPR)
- ISO/IEC 27001
- SOC 2 Compliance

01

REGULAR AUDITS AND ASSESSMENTS

Conducting periodic internal or external audits to assess compliance with our policies, standards, and regulatory requirements.

02

CONTINUOUS MONITORING

Providing ongoing training and resources to our employees to foster a culture of security awareness and ensure that all team members are informed of their roles in maintaining compliance.

03

EMPLOYEE TRAINING AND AWARENESS

Implementing advanced monitoring tools and techniques to detect and respond to security incidents and compliance deviations in real-time.

04

STAKEHOLDER ENGAGEMENT

Engaging with clients, partners, and regulatory bodies to transparently communicate our compliance status and address any concerns or requirements they may have.

DATA PROTECTION AND PRIVACY

In the digital age, the protection of data and the privacy of individuals are paramount. At Novacore AI, we understand that the trust our clients place in us is contingent on our ability to secure their data and uphold the confidentiality and integrity of their information. This section delves into our rigorous data protection and privacy practices, demonstrating our unwavering commitment to safeguarding data at every juncture of our operations.

DATA MINIMIZATION

We adhere strictly to the principle of data minimization, collecting only the data necessary for the specific purposes for which it is processed. This approach extends to our AI and vision model-based document verification services, where data processing is executed **on-the-fly**, without retaining personally identifiable information (PII).

TRANSPARENCY

We maintain a policy of transparency about the data we collect, how it is used, and the measures we take to protect it. Clients are informed of our data handling practices through clear and accessible policies.

SECURITY BY DESIGN AND DEFAULT

Our systems and processes are engineered with security in mind as a foundational element, ensuring that personal data is protected using appropriate technical and organizational measures from the outset.

DATA PROCESSING AND HANDLING

ON-THE-FLY PROCESSING

Our platform is designed to process documents and verify their authenticity in real-time, ensuring that no sensitive data is stored on our systems beyond the duration of the transaction. This approach minimizes the risk of data breaches and unauthorized access.

NON-PII METADATA STORAGE

The only data retained post-processing is non-personally identifiable information metadata, used solely for invoicing purposes and operational analytics. This data is stored with the highest level of security and privacy protections, following best practices in data encryption and access control.

NOT USING CUSTOMER DATA FOR TRAINING

NovaCore Ai and its sub-processors do not store, use or utilize our customer data for training AI models or any similar activity.

DATA ENCRYPTION AND SECURITY MEASURES

ENCRYPTION AT REST AND IN TRANSIT

We employ advanced encryption protocols to protect data at rest and in transit. Utilizing Azure's comprehensive security features, data is encrypted using industry-standard methods, ensuring its confidentiality and integrity.

AZURE SECURITY PRACTICES

Hosted on Azure US East 2, our platform benefits from Microsoft's robust security infrastructure. We leverage Azure's built-in security features, including network security, threat protection, and identity and access management, to enhance our data protection capabilities.

PRIVACY COMPLIANCE AND RIGHTS

REGULATORY COMPLIANCE

We ensure our data handling practices are in full compliance with applicable laws and regulations, such as the General Data Protection Regulation (GDPR) for European clients. This includes respecting users' rights to access, rectify, and erase their personal data, along with rights to data portability and objection to processing.

DATA RETENTION AND DELETION POLICIES

Our data retention policies are crafted to hold data only as long as necessary for the purposes for which it was collected or as mandated by law. Upon the expiration of this period, data is securely deleted or anonymized.

> At Novacore AI, data protection and privacy are not just regulatory requirements but core values that guide our operations and interactions with clients. By implementing rigorous data protection measures and respecting the privacy of individuals, we aim to foster a secure and trustworthy digital environment for businesses worldwide.

Physical and Network Security

Ensuring the security of our physical and digital environments is paramount at Novacore AI. This commitment is evident in our comprehensive approach to physical and network security, designed to protect our infrastructure, data, and assets from unauthorized access, damage, or theft. This section outlines our strategies and measures in place to secure our physical premises and safeguard our network infrastructure.

Network Security Architecture

NETWORK SEGMENTATION

Our network is segmented into distinct zones, using firewalls and virtual private networks (VPNs) to separate sensitive areas and minimize the potential impact of security breaches.

DATA ENCRYPTION

All data transmitted across our network or stored on our systems is encrypted using strong cryptographic standards, ensuring that data remains confidential and protected against unauthorized access.

INTRUSION DETECTION AND PREVENTION SYSTEMS

We utilize IDPS to monitor network and system activities for malicious actions or policy violations, with automated responses to detected incidents to mitigate threats.

REGULAR SECURITY ASSESSMENTS

We conduct regular security assessments, including vulnerability scans and penetration testing, to identify and address potential vulnerabilities within our network infrastructure.

Hosted Environment Security

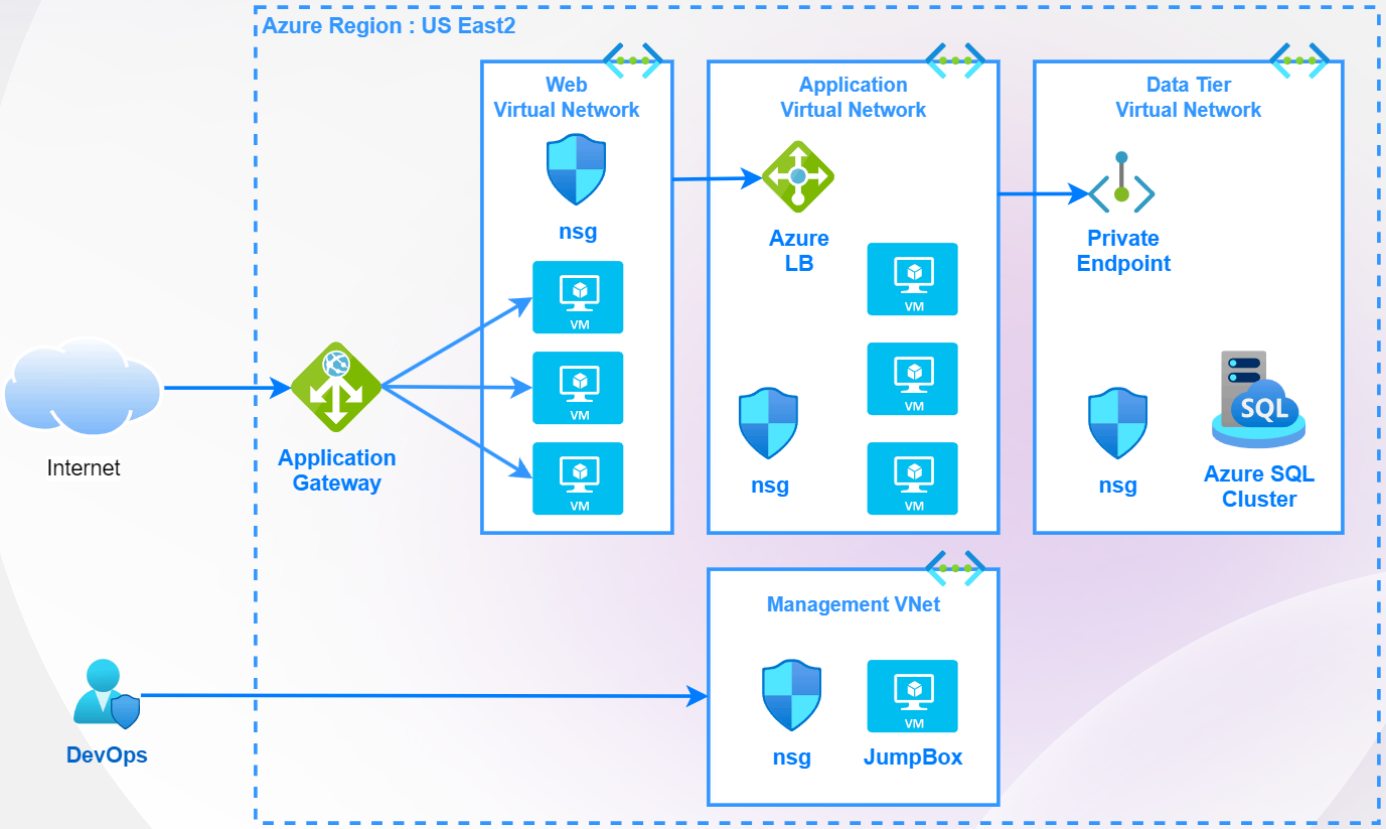
Our platform is hosted on Azure US East 2, benefiting from Microsoft Azure's comprehensive security infrastructure

AZURE SECURITY FEATURES

We leverage Azure's advanced security tools, such as Azure Security Center, and Azure Firewall to enhance our security posture. These tools provide continuous security monitoring, threat detection, and automated threat response capabilities.

COMPLIANCE WITH AZURE STANDARDS

Our use of Azure services adheres to Microsoft's strict security standards and compliance certifications, ensuring that our hosted environment is secure, resilient, and compliant with industry regulations.



Access Control and Identity Management

At Novacore AI, securing sensitive information and critical infrastructure begins with robust access control and identity management practices. These practices are central to our security strategy, ensuring that only authorized individuals can access specific data and systems within our network. This section delves into the measures and methodologies we employ to maintain strict access control and manage identities effectively.

FOUNDATIONAL PRINCIPLES

LEAST PRIVILEGE

We adhere to the principle of least privilege, ensuring that individuals are granted access only to the information and resources necessary for their specific roles. This minimizes potential exposure to sensitive data and systems.

ROLE-BASED ACCESS CONTROL (RBAC)

Access rights are assigned based on roles within the organization, facilitating granular control over who can view, modify, or interact with certain data or systems. RBAC policies are regularly reviewed and updated to reflect changes in roles or responsibilities.

AUTHENTICATION AND AUTHORIZATION

We implement stringent authentication mechanisms, including multi-factor authentication (MFA), to verify the identity of users attempting to access our systems. Following successful authentication, authorization processes determine the resources and operations accessible to the user.

IDENTITY MANAGEMENT PRACTICES

Effective identity management is crucial for maintaining operational security and integrity. Our practices in this area include

CENTRALIZED IDENTITY REPOSITORY

Utilizing Azure Active Directory (AD), we maintain a centralized repository of user identities, streamlining the management of user attributes, credentials, and access rights

LIFECYCLE MANAGEMENT

We manage the entire lifecycle of user identities, from onboarding to offboarding, ensuring that access rights are appropriately assigned at the outset and promptly revoked when no longer needed.

REGULAR AUDITS AND REVIEWS

To prevent unauthorized access and ensure compliance with our access control policies, we conduct regular audits and reviews of user accounts and access rights. Any anomalies or unnecessary privileges are swiftly addressed.

> Access control and identity management are critical components of Novacore AI's overall security posture. By implementing rigorous controls, managing identities effectively, and leveraging advanced technologies, we ensure that our systems and data remain secure against unauthorized access. Our commitment to these practices underscores our dedication to protecting the privacy and integrity of the information entrusted to us by our clients.

SECURE AUTHENTICATION TECHNOLOGIES

MULTI-FACTOR AUTHENTICATION

MFA is mandatory for accessing our critical systems, adding an extra layer of security by requiring two or more verification factors, which significantly reduces the risk of unauthorized access.

SINGLE SIGN-ON

SSO enables users to access multiple applications or services with a single set of credentials, improving user experience while maintaining security through centralized authentication controls.

Continuous Improvement

SECURITY AWARENESS TRAINING

TECHNOLOGY AND POLICY UPDATE CYCLE

FEEDBACK LOOPS AND INCIDENT ANALYSIS

COMMITMENT TO EXCELLENCE

At Novacore AI, our journey towards achieving and maintaining the highest levels of security and compliance is perpetual. We recognize that in the rapidly evolving digital landscape, excellence in security is not a destination but a continuous journey. Our commitment extends beyond the implementation of robust security measures; it encompasses a culture of vigilance, adaptability, and transparency.

FOSTERING TRUST AND CONFIDENCE

The trust our clients place in us is not taken lightly. It is the foundation upon which we build our relationships and our business. By providing a transparent view into our security and compliance practices, we aim to foster a deep sense of trust and confidence among our clients, partners, and stakeholders. Our dedication to maintaining a secure and compliant environment ensures that our clients can rely on Novacore AI to protect their most valuable digital assets.

LOOKING FORWARD

As we look towards the future, We will continue to invest in the latest technologies, engage with industry experts, and adhere to best practices to enhance our security posture. Our proactive approach to addressing emerging threats and vulnerabilities ensures that we are well-equipped to navigate the complexities of the digital age, while supporting our clients in achieving their business objectives with confidence.

INVITATION FOR CONTINUOUS DIALOGUE

We view security and compliance as a collaborative effort, requiring ongoing dialogue and cooperation between Novacore AI and its clients, partners, and the broader community. We welcome feedback, inquiries, and discussions on how we can collectively enhance our security practices for the mutual benefit of all parties involved.

Thank you for taking the time to review our Security and Compliance Framework. We look forward to continuing to serve as your trusted partner in securing your digital journey.

www.novacore.ai
success@novacore.ai