NEXTWORLD

Ahead of the Next Threat

RELATIONSHIPS ARE BUILT ON TRUST. At Nextworld®, we recognize that a key component to that trust is the responsibility we have to our customers information security and privacy. We place a priority on security and continually invest in the Nextworld ERP platform that provides you with industry-leading security and privacy capabilities.

nextworld®
ERP Redefined

IT BEGINS WITH PEOPLE

INFORMATION SECURITY MEASURES are only as good as the people behind them. Nextworld® has implemented a number of policies, procedures, and controls to govern how our staff protect the information entrusted to us. This includes every employee completing training courses on our information security policies, procedures, and cyber security upon hire and every subsequent year of their employment. In addition, a background check is conducted on every prospective employee and confidentiality agreements are in place for each new employee. Finally, Nextworld has appointed a senior resource that is accountable and responsible for our security and privacy programs. At Nextworld, data protection is not just about making regulators happy or achieving certificates. It is part of our culture to be a fantastic business partner.

KEEPING THE BAD GUYS OUT

A KEY COMPONENT in maintaining the confidentiality and integrity of your data is controlling who has access to it. Access control is a shared responsibility between Nextworld and you the customer. Nextworld is responsible for preventing unauthorized external access to the data while giving you complete control over who has access to the data. In other words, Nextworld builds the fortress and provides you the keys to the gate.

BUILDING THE FORTRESS

NEXTWORLD TAKES A MULTIPLE-LAYERED APPROACH to security to ensure your data is protected. The Nextworld database is never exposed to the public internet and cannot be accessed externally - outside of the Nextworld internal cloud. Only the runtime components in the API layer can access the Nextworld Database that can only be accessed through the REST interface. This interface also encrypts your data as it moves through the Nextworld system while database encryption protects your data at rest. We use a multi-tenant model with data encapsulation to segregate individual customer tenants. This model allows us to effectively manage the cloud infrastructure to optimize performance and availability while giving you complete control of your data.

Nextworld architecture leverages Amazon Web Services (AWS), a pioneer and industry leader in cloud computing, for our infrastructure services to provide further access protections. We have implemented Geo Blocking to restrict access for high threat areas.

P +1 303.903.3345 | info@nextworld.net | nextworld.net | ©2022

KEYS TO THE GATE

THE NEXTWORLD® PLATFORM gives you complete control over who accesses your data with comprehensive security capabilities. These capabilities allow you to control access to your Nextworld environment and the data inside of it. It starts with our authentication model that includes the following capabilities:

- Multi factor authentication – SMS and authenticator app capabilities
- Single sign-on support
- Complete tenant-defined password complexity rules
- Highly secure one-way hash for passwords – no password storage or recoverability
- Forced password expiration
- End user password reset
- Failed login attempts tracked and resulting in disabled logins
- Failed login attempts tracked and resulting in disabled logins
- IP whitelisting
- Advanced token management – based authentication model with frequently changing keys and key sizes

Nextworld also offers an extensive and unified authorization model. This model adheres to the principle of least privilege. Nextworld assumes users have access to no resources until explicitly given permission. Access is granted only through explicitly defined Security Groups. Roles and permissions built on these Security Groups are designed such that users have access to the minimal resources necessary. This authorization model is fully defined in the Nextworld metadata model and completely enforced by the Nextworld runtime engine. These capabilities coupled with the fact that the Nextworld production database is not directly accessible ensures that all permission rules are always enforced.

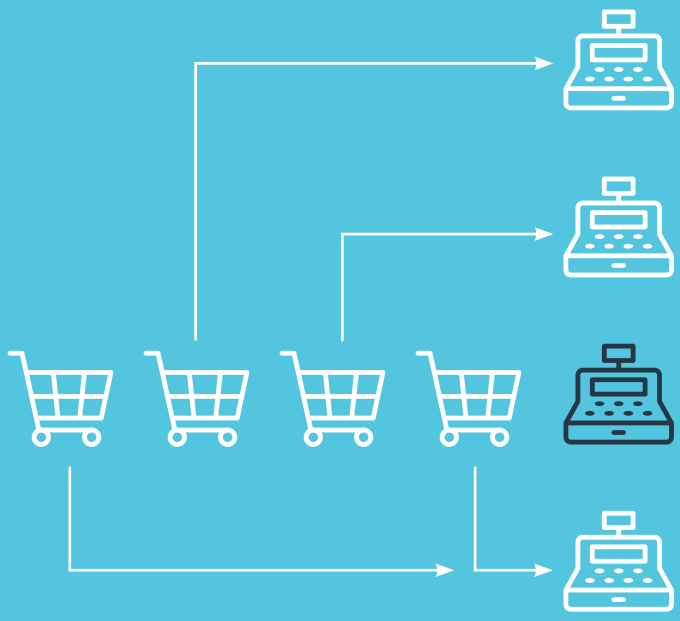
Nextworld further provides security at the individual data item level. Nextworld field level security can lock down any personally identifiable information (PII) or sensitive field. It is also configurable such that this information may be either masked, completely hidden, viewable but not changeable, etc.

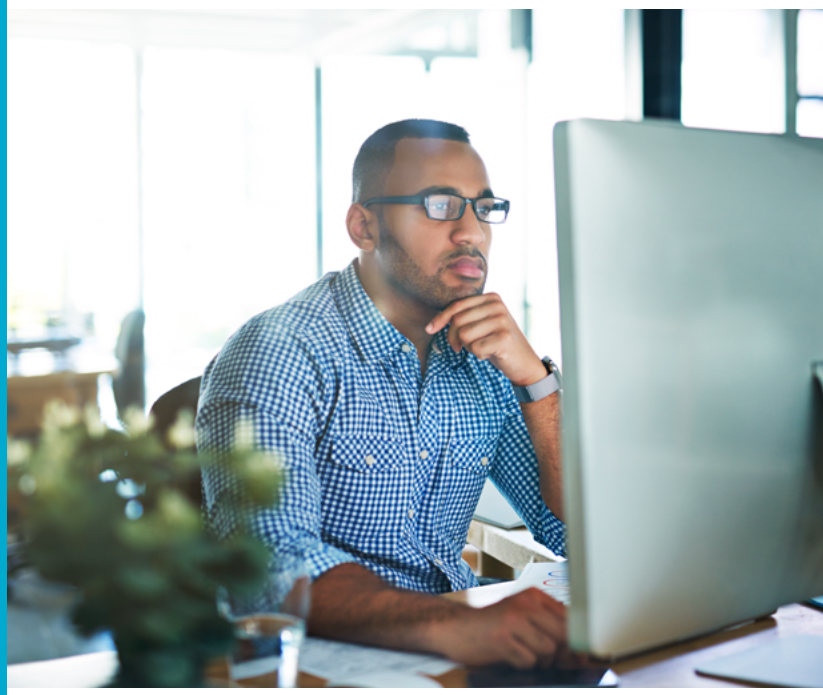
The Nextworld Platform gives you complete control over who accesses your data with comprehensive security capabilities. These capabilities allow you to control access to your Nextworld environment and the data inside of it.

DISASTER RECOVERY THAT PROVIDES CONFIDENCE

DISASTERS NEVER HAPPEN. Don't you wish this were true? What is true is that Nextworld® services insulate you from disasters. Nextworld tackles disaster recovery by focusing first on the preservation of work, and second, on how we restore operations.

All Nextworld servers are stateless and distributed across different data centers. Think of statelessness as checking out at the grocery store where the shopping cart is your data, and the cash register is the service. If there is only one cash register, your ability to complete your shopping is dependent on the single cash register. A failure in that cash register forces you to lose all the work you did collecting the items you wanted to buy and start the process all over at another store. If a cash register fails at a store with multiple cash registers, your cart is routed to a different register to complete your transaction.





This statelessness results in no loss of work or data corruption due to any server failures. Only the production databases maintain any state and as these are replicated in real time in a separate data center. Nightly backups are also performed and replicated is a separate AWS region. This combination of stateless servers and real-time replication of the production database, allows us to provide near-instance, real-time disaster recovery and failover without you being aware an incident has occurred.

What is true is that Nextworld services insulate you from disasters. Nextworld tackles disaster recovery by focusing first on the preservation of work, and second, on how we restore operations.

P +1 303.903.3345 | info@nextworld.net | nextworld.net | ©2022

TRUST BUT VERIFY

NEXTWORLD® ENGAGES WITH THIRD PARTIES to conduct independent audits and assessments of our information security and privacy measures. An external auditing firm conducts an annual AICPA Service Organization Control Report 1, Type II and Report 2, Type II (SOC 1 and SOC 2, Type II). In addition to the SOC reports we have had third-party assessments conducted against our information security and data privacy practices to evaluate our compliance to various regulatory and industry standards, such as the European Union's General Data Protection Regulation (GDPR) and the NIST Cybersecurity Framework and Privacy Framework.

WE VALUE YOUR INFORMATION

INFORMATION IS VALUABLE and as with anything that has value, there will always be risks associated with it. Nextworld wants to honor your investment with us by providing you a secure ERP system across your enterprise that exceeds your expectations of reasonable security measures. The intent of this document is to give you an idea of how Nextworld aims to meet those expectations. Our culture places a premium on relationships, therefore our approach to security is about furthering our relationship with you and being a fantastic business partner. If you have questions regarding Nextworld's security practices, please contact our **Sales Team**.