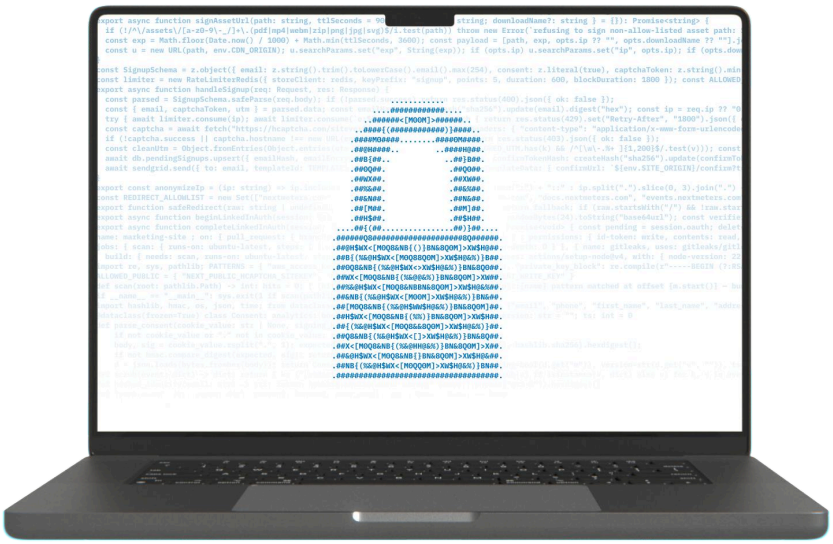
NextCity

Cybersecurity & Disaster Recovery



Platform Security

Protecting Data at Every Layer

NextCity is built to meet the strict security needs of modern utilities, ensuring critical utility data remains safe, private, and accessible. Security protections extend from field devices and communications to cloud infrastructure, user access, and disaster recovery.

Secure Hardware

Next Meters products are designed to prevent tampering at the hardware level. Each device is potted, sealing the internal components to block access to the circuit board. This design helps prevent both accidental and intentional interference, safeguarding against unauthorized firmware changes, parameter adjustments, or clock manipulation.

Field devices transmit meter readings and operational health information, such as battery level and signal strength. They do not transmit customer names, addresses, or payment information.

Device Communications

Current-generation devices encrypt each message using AES-256-CCM, providing confidentiality, integrity, and authenticity. Each device uses its own encryption key, so the compromise of one device's key would not affect other meters.

On supported firmware, commands sent to meters receive the same encryption and integrity protection. This allows devices to detect and reject commands that have been altered in transit.

Cybersecurity & Disaster Recovery

Firmware Updates
Firmware updates are developed and released through Next's controlled deployment process. Updates are delivered with integrity checks applied to individual sections and the complete firmware image. Before activating an update, the device verifies that the entire image arrived correctly and without unauthorized modification.

Data Encryption
Connections between users' browsers and NextCity are encrypted using HTTPS/TLS. Readings transmitted by current-generation meters are also encrypted as they travel across cellular networks to the NextCity platform.

Once in the cloud, device messages and stored files are protected with AES-256 encryption in private Amazon S3 buckets and encrypted Amazon SQS queues. Databases hosted on AWS use encrypted Amazon EBS volumes, providing a high level of protection for stored information.

Secure Cloud Storage & Processing
NextCity runs on Amazon Web Services (AWS), which provides the physical and network infrastructure supporting the platform. AWS maintains independent certifications and audit programs, including SOC 2 and ISO 27001.

NextCity databases, caches, and file storage operate within a private AWS network and are not directly accessible from the public internet. Access is limited to authorized application services and administrative personnel. Device messages are processed through private cloud workloads, helping protect customer information throughout collection, processing, and storage.

Web Portal Security
Traffic to NextCity is protected by an AWS web application firewall, which helps identify and block common malicious requests before they reach the platform.

Access to the web portal is controlled through authentication middleware and role- and claim-based authorization. Users may sign in using supported account credentials or approved identity providers. Sessions expire automatically and can be revoked, helping prevent continued access when credentials or devices are no longer authorized.

File downloads use temporary links that expire after a limited period. API credentials used for approved integrations are stored securely, may be revoked or configured to expire, and are never stored in plain text.

Role-Based Access & Utility Separation
Each utility controls who is authorized to access its NextCity account. Users are assigned roles based on their responsibilities, ensuring they can see and perform only the actions their role allows.

Every request is checked against both the user's permissions and the utility to which the user belongs. This separation prevents one utility's users from accessing another utility's data. When authorization cannot be verified, access is denied.

Disaster Recovery

Backups, Redundancy & Recovery
NextCity leverages the reliability and redundancy of Amazon Web Services to support continued operation and rapid recovery in the event of a system disruption.

NextCity data is backed up automatically using daily, weekly, and monthly snapshots. Daily backups are retained for seven days, weekly backups are retained for five weeks, and monthly backups are retained for twelve months. These procedures support data restoration following accidental deletion, system failure, or a ransomware-style event.

AWS data centers are designed to accommodate failure while maintaining service levels. When disruptions occur, automated processes reroute traffic to support continued operation. Core applications are deployed to an N+1 standard, providing sufficient capacity for load balancing in the event of a data center outage.

System Monitoring & Incident Response
NextCity employs AWS CloudWatch and other monitoring tools to track system performance and behavior across the platform and meter network. Dashboards, key metrics, automated alerts, and activity logs help the internal admin team identify unusual behavior and respond to issues as they arise.

Access to production infrastructure is limited to authorized Next Meters personnel and protected with multi-factor authentication. Software changes are reviewed and tested before release, and controlled, automated deployment processes help reduce the risk of unauthorized or unintended changes.

Auditability & Record History
NextCity maintains an audit history of changes to customer records. Audit information includes the acting user, the time of the change, and relevant change details. Actions taken by authorized Next Meters support personnel while assisting a utility are also recorded.

Deleted records are removed from normal use while appropriate change history is retained. This allows mistakes or unexpected activity to be investigated, traced, and corrected.

Data Privacy & Access Control
NextCity uses best-practice password policies for client logins and enforces multi-factor authentication for internal administrative access to its infrastructure. Strict authorization, utility-level separation, and comprehensive logging ensure that access to customer data remains controlled, auditable, and secure.

Customer data remains the sole property of the utility and is used only to provide and support the NextCity service. Next Meters does not sell customer data or share it with third parties for their own independent use.

Cybersecurity & Disaster Recovery

Security Standards
Next's security practices are guided by widely recognized frameworks, including the NIST Cybersecurity Framework and the risk and resilience principles of America's Water Infrastructure Act. NextCity also benefits from AWS infrastructure supported by independent certifications and audit programs, including SOC 2 and ISO 27001.

Shared Responsibility
Security is a shared responsibility. Utilities can help protect their information by promptly removing accounts when employees leave or change responsibilities, assigning each user the lowest level of access needed, providing each user with a unique login and using strong, unique passwords or approved identity providers with multi-factor authentication.

Utilities should report unexpected emails, unfamiliar account activity, or other suspicious behavior to Next Meters as soon as possible.

Summary

Secure, Reliable, & Ready for the Future
By combining secure field devices, per-device encryption, private cloud infrastructure, role-based access controls, utility-level data separation, system monitoring, and robust backup procedures, NextCity provides a highly secure and resilient platform for utilities and their customers.

From device data collection and firmware delivery to cloud storage and web access, every layer of NextCity is designed with security, privacy, redundancy, and disaster recovery in mind.

Want to know more?

Contact us to learn more about our cybersecurity procedures.

nextcitysupport@nextmeters.com

(844) 538-8203
6am–6pm MT, Mon-Fri