SECURITY STANDARDS
URBI GULF FZ-LLC

Version as of January 29, 2026

URBI Gulf FZ-LLC implements comprehensive technical and organizational measures to ensure the security of its software platforms, geospatial data, analytics modules, and cloud infrastructure. Information security is considered an integral part of the platform architecture, development processes, operational practices, and interactions with clients and partners.

These Security Standards define the core principles according to which URBI ensures data protection, access control, platform resilience and reliability, and the prevention of unauthorized use of URBI technologies, services, and data. These principles apply to all systems, services, APIs, data, and infrastructure used in the company's operations and form part of URBI's overall approach to risk management, information protection, and business continuity.

Access Control and Role-Based Access (RBAC)

Access to URBI systems, data, platform modules, and administrative functions is granted strictly on a need-to-know and least-privilege basis. URBI applies a Role-Based Access Control (RBAC) model, where user permissions are determined by functional role and job responsibilities.

Procedures for granting, modifying, and revoking access are formalized and carried out through a controlled approval process. Access is provided only to authorized users based on approved requests and is properly recorded.

URBI ensures:

- unique user identification and controlled authentication mechanisms;
- clear separation between user, administrative, and technical access;
- restriction and control of privileged access;
- regular review and update of access rights;
- immediate revocation of access upon change of role or termination of engagement;
- logging of user access and activities for audit and monitoring purposes.

This access control model is designed to prevent unauthorized access to systems, data, and platform functions, and to ensure accountability and traceability of user actions.

Data Encryption

URBI ensures the protection of data through the use of modern encryption methods and technical safeguards both in transit and at rest.

Data transmitted between users, services, and infrastructure is transferred through secure communication channels using up-to-date cryptographic protocols. This prevents interception or unauthorized modification of data during transmission.

Data storage, including geospatial data, analytics data, user information, and backups, is maintained in encrypted form. Cryptographic protection is applied to databases, file storage systems, and backup repositories, reducing the risk of unauthorized access to information even in the event of physical or logical access to the infrastructure.

Access to encryption keys is restricted and controlled, and the keys themselves are stored and managed within a secure environment.

These measures are aimed at ensuring the confidentiality and integrity of data throughout all stages of processing and storage within URBI systems.

Secure Software Development

In the development of its software platforms, web interfaces, and APIs, URBI applies secure development practices as part of its overall software development and maintenance process.

Security is considered at the stage of architecture design, feature development, and ongoing system maintenance. Approaches are applied to prevent common vulnerabilities in web applications, APIs, and server-side logic.

URBI ensures:

- the use of secure coding principles during software development;
- internal review and testing of software components prior to deployment;
- proper validation and handling of user input and requests;
- restriction and protection of APIs against unauthorized use;
- regular review and updating of software components to address potential vulnerabilities.

URBI performs periodic internal security testing of its applications and APIs, including vulnerability assessments and controlled security checks aimed at identifying and mitigating potential weaknesses.

These measures reduce the risk of vulnerabilities within the platform and enhance the resilience of URBI's software solutions against common types of attacks.

Logging and Monitoring

Key user actions, administrative operations, data access events, and system activities are recorded in event logs. URBI maintains audit trails for the purpose of subsequent analysis and control.

Event logs are stored in a secure environment with restricted access. These records are used to monitor the proper functioning of the system, detect abnormal activity, and support the investigation of potential security incidents.

Security Incident Management

URBI applies internal procedures for the timely identification, containment, and resolution of information security incidents. These procedures include prompt measures to limit potential impact, analysis of the root cause of incidents, and implementation of actions to prevent recurrence.

As part of incident management, coordination among responsible personnel is ensured, and key stages of the response process are properly documented.

Cloud and Server Infrastructure Security

The URBI platform is hosted within a secure cloud and server infrastructure with restricted and controlled access to servers and system components. Network segmentation, environment separation, and continuous infrastructure monitoring are applied to ensure the protection of systems and services.

Access to infrastructure components is limited to authorized personnel only and is subject to strict access control procedures. Infrastructure environments are logically separated to reduce risks of unauthorized access and cross-environment impact.

Infrastructure components are regularly updated, patched, and maintained to ensure the stability, reliability, and security of the platform.

These measures are implemented in accordance with applicable information security and cybersecurity requirements under the laws of the United Arab Emirates, including **Federal Decree-Law No. 34 of 2021 on Personal Data Protection**, **Federal Decree-Law No. 26 of 2019 on Combating Cybercrimes**, and relevant regulatory requirements concerning the protection of information systems and infrastructure.

Protection of Data and Geospatial Information

URBI applies comprehensive technical and organizational measures to protect geospatial data, analytics data, and client information from unauthorized access, alteration, loss, or distortion.

Data processing and storage are carried out in accordance with the principles of confidentiality, integrity, and availability of information throughout the entire data lifecycle. These measures are designed to ensure that data remains protected during collection, processing, storage, transmission, and backup.

URBI's approach to data protection is aligned with applicable data protection and information security requirements under **Federal Decree-Law No. 34 of 2021 on Personal Data Protection** and related regulatory provisions of the United Arab Emirates governing the protection of data and information systems.

Internal Security Procedures

URBI employees are required to comply with confidentiality obligations and internal information security rules. Access to internal systems and data is controlled and granted in accordance with established procedures.

URBI regularly reviews and updates the security measures in place, taking into account technological developments, emerging risks, and evolving information security practices.

Security Governance and Continuous Improvement

URBI treats information security as an ongoing process. Security measures, procedures, and technical controls are periodically reviewed, tested, and improved in line with evolving risks, technologies, and best practices.

These Security Standards are developed in accordance with applicable requirements in the field of information security and data protection and are based on internationally recognized information security standards, including the principles of the ISO/IEC 27000 series, as well as industry best practices for technology and data service providers.

These Standards apply to all URBI platforms, services, systems, and data and are to be observed by employees, users, and partners where applicable.