THIRD-PARTY SECURITY STANDARD
URBI GULF FZ-LLC

Version as of February 2, 2026

URBI Gulf FZ-LLC recognizes that cyber security risks may arise not only from its own systems, but also from third parties interacting with URBI platforms, data, APIs, infrastructure, or services.

This Standard applies to all persons interacting with URBI systems, platforms, data, or infrastructure, including contractors, consultants, integrators, developers, cloud and hosting providers, data providers and analytics partners, clients and partners with system or API access, support providers, and other service vendors (hereinafter collectively referred to as the "Third Parties").

1. **Risk Classification**

This Standard is aligned with the UAE Cyber Security Council National Third Party Security Policy (2025) and forms part of URBI's overall information security and risk management framework.

URBI maintains a register of third-party suppliers and classifies them according to their level of access and risk exposure:

Low Risk — no system or data access.

Medium Risk — limited technical or data interaction;

High Risk — access to systems, data, infrastructure, or production environments;

Security controls and oversight are applied proportionally to the risk level.

*High-Risk Supplier Requirements**

For Third Parties classified as High Risk, URBI may apply enhanced security and oversight measures, including, but not limited to:

- *additional due diligence and security questionnaires;*
- *provision of security policies, certifications, or assessment reports;*
- *verification of incident response capabilities;*
- *stricter access limitations and monitoring;*
- *periodic compliance confirmations;*
- *remote or on-site security reviews where necessary.*

2. **Third-Party Security Assessment**

Prior to granting access to URBI systems or data, URBI may assess the cyber security posture of the third party, including:

- information security practices;
- data protection measures;
- access control practices;
- incident response capability.

URBI reserves the right to request confirmation of such measures.

3. **Security Requirements for Third Parties**

Third Parties shall ensure compliance with the following information security and cyber security requirements:

3.1 Account and Access Management

Third Parties shall ensure proper management of user accounts and access to URBI systems. Access must be granted strictly on a need-to-know basis and limited to authorized personnel within the scope of their job responsibilities. Individual user accounts must be used at all times, and the use of shared accounts or sharing of credentials is strictly prohibited.

Third Parties must maintain an internal record of personnel with access to URBI systems and ensure that access is immediately revoked upon change of role or termination of employment. Strong authentication measures, including complex passwords and, where possible, multi-factor authentication, must be applied.

3.2 Protection of Devices and Workstations

Access to URBI systems shall be performed only from secured and properly maintained devices. Third Parties must ensure that operating systems and software are regularly updated with the latest security patches and that appropriate antivirus and endpoint protection measures are in place.

When accessing URBI systems, secure network connections must be used, and unsecured public networks should be avoided.

3.3 Handling of URBI Data

Third Parties are responsible for ensuring the secure processing, storage, and transmission of URBI data. Data must be transmitted only through secure communication channels such as HTTPS, VPN, or equivalent protections.

URBI data must not be copied, transferred, or used outside the agreed purposes of engagement and must not be stored on unsecured devices or media.

3.4 Internal Information Security Measures

Third Parties shall implement internal confidentiality and information security rules applicable to personnel with access to URBI systems and data. Employees must be informed of their data protection and confidentiality obligations, and access to URBI data must be restricted to a defined group of authorized individuals.

3.5 Traceability and Control of Actions

Third Parties must ensure traceability of access to URBI systems and data, allowing identification of which personnel accessed systems and at what time. Appropriate internal controls over the use of such access must be maintained.

3.6 Incident Response

Third Parties shall maintain internal procedures for responding to information security incidents and must immediately notify URBI of any suspected incident, data breach, or unauthorized access. Prompt measures must be taken to contain and mitigate the impact of such incidents.

3.7 Software, Components and End-of-Life Considerations

Where Third Parties provide software, integrations, components, or technical services:

- they must notify URBI of relevant vulnerabilities, updates, and security patches;
- ensure supported and maintained software versions;
- inform URBI of end-of-life (EOL) status of any component affecting URBI services;
- ensure secure decommissioning and protection of URBI data upon end of service life.

3.8 Compliance with Legal and Contractual Obligations

Third Parties are required to comply with applicable data protection and cybersecurity laws, as well as all contractual obligations related to confidentiality, data protection, and information security.

3.8 End of Engagement

Upon completion or termination of engagement, Third Parties must return or securely delete URBI data, cease access to URBI systems, and confirm completion of these actions upon request.

---

4. Monitoring and Audit

URBI reserves the right to monitor access to its systems, maintain audit logs, and verify Third Parties' compliance with contractual and established security requirements.

For this purpose, URBI may request confirmations, supporting documentation, written explanations, or evidence of implemented security measures from Third Parties, including via official correspondence. Where necessary, URBI may also conduct reviews of access records, request security self-assessments, or require confirmation of compliance with the obligations set out in this Standard.

Higher-risk suppliers may be subject to enhanced oversight, additional verification measures, and more frequent compliance checks.

5. Governance and Continuous Improvement

URBI treats third-party security as an ongoing process. Supplier risks, control measures, and security requirements are periodically reviewed and updated in line with evolving cybersecurity practices and applicable regulatory expectations in the United Arab Emirates.