VIDIZMO.AI

VIDIZMO SECURITY OVERVIEW

Last Updated: August 2025

TABLE OF CONTENT

VIDIZMO SECURITY AND RISK FOCUS

VIDIZMO's primary security focus is to safeguard Customer Data across our SaaS products. This is why we invest in the people, processes, and controls needed to protect our customers and deliver reliable, secure services. Dedicated Information Security and Product Security teams lead our comprehensive security program and governance. We focus on defining and refining controls, operating a strong security framework, and supporting effective risk management across the company. Security oversight is provided by our information security leadership to ensure safeguards are applied consistently across all VIDIZMO platforms.

OUR SECURITY AND RISK MANAGEMENT OBJECTIVES

At VIDIZMO, security is a promise we keep every day. Our program is built around clear, human goals that guide how we design, run, and improve our products.

- Protect customer trust - safeguard the privacy and confidentiality of Customer Data at every step.
- Be reliably available - keep services up and data accessible to authorized users when they need it.
- Preserve integrity - ensure information stays accurate, complete, and unaltered.
- Follow proven standards - align our controls with leading frameworks like ISO 27001 and SOC 2, and support compliance needs for GDPR, CCPA, CJIS, and HIPAA.
- Keep access minimal - enforce MFA, SSO, and role-based access so people only see what they need to do their jobs.
- Improve continuously - review risks, test often, learn from every event, and strengthen our policies and controls over time.

1. DATA SECURITY AND GOVERNANCE

1.1. Purpose, Scope and Audience

This overview explains how VIDIZMO protects Customer Data across our SaaS products (EnterpriseTube, VIDIZMO DEMS, VIDIZMO Redactor, and AI Platform). It applies to customers, partners, and VIDIZMO personnel who handle Customer Data and outlines the controls we use to safeguard it and support compliance with GDPR, CCPA, and other applicable regulations.

1.2. Governance and Security Frameworks

VIDIZMO SaaS is hosted on Microsoft Azure cloud, whose underlying infrastructure meets rigorous standards (e.g., ISO 27001, SOC 2 Type II, and NIST).

For more information on Microsoft Azure compliance, please visit Azure compliance documentation | Microsoft Learn.

VIDIZMO is ISO 27001 certified and maintains a formal Information Security Program with regular risk assessments, audits, and policy reviews to keep controls effective and current.

We support customers' compliance needs, including:

- GDPR (EU)
- CCPA (California, USA)
- CJIS (U.S. criminal justice workloads)
- HIPAA (U.S. healthcare workloads)

1.3. Access Control and Identity Management

VIDIZMO uses Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Role-Based Access Controls (RBAC) to protect access to Customer Data. Access is provisioned on a least privilege, need-to-know basis, so only authorized users can view or modify information. All activity is logged and monitored for suspicious behavior, and audit trails are retained to provide transparency and demonstrate compliance.

1.4. Audit and Compliance Verification

1.4.1. Annual Right to Audit

The Controller or Processor may conduct an annual review of Vidizmo.ai's compliance with this Agreement.

1.4.2. Permissible Audit Methods

To protect continuity of service and security, audit activities are limited to one or more of the following:

- Meetings between Vidizmo.ai and the Controller, Processor, or their designated representatives.
- Completion of audit-related questionnaires by Vidizmo.ai.
- Provision by Vidizmo.ai of information or documentation sufficient to demonstrate compliance with this Agreement.

1.4.3. Scope and Limitations

Vidizmo.ai is not required to disclose sensitive internal documentation, proprietary controls, or internal reports where disclosure could compromise confidentiality, security, or business interests. All audit activities are subject to reasonable limits and, where appropriate, a mutual non-disclosure agreement.

1.4.4. Cooperation and Regulatory Support

Vidizmo.ai will cooperate in good faith with audit requests, including providing reasonable support for Data Protection Impact Assessments (DPIAs) and regulatory consultations, as required by applicable law or regulation.

1.5. Audit Logging and Monitoring

VIDIZMO implements real-time monitoring and audit logging for all security-related activities on the platform. All interactions with Customer Personal Data are logged, providing full traceability and accountability. These logs are stored in WORM-enabled storage to maintain their integrity, ensuring that they cannot be tampered with. Logs are regularly reviewed to detect any suspicious or unauthorized access, supporting compliance and security audits

1.6. Security Awareness Training

We view our employees as the first line of defense, and we make sure VIDIZMO teams are prepared for that role. New hires complete core security awareness training at onboarding, with a required annual refresher that covers current best practices and policy updates. We also share timely security news and initiatives through internal communications and knowledge articles.

Beyond the basics, employees receive role-based training tied to their responsibilities and access levels. Product and engineering teams, for example, take secure development training focused on common risks, threats, and preventive controls.

1.7. Policy Management and Updates

VIDIZMO conducts regular reviews and updates of this Data Security Policy to ensure its effectiveness and alignment with evolving regulatory requirements and industry best practices. Version control is maintained to track changes and ensure that all stakeholders are informed of updates. Ongoing compliance with data protection laws and security frameworks is ensured through these periodic revisions.

2. DATA PROTECTION AND PRIVACY

VIDIZMO has stringent data protection and privacy measures—including strong encryption (at rest/in transit), MFA/SSO with RBAC, continuous audit logging/monitoring, and strict data retention/deletion controls. For more information, please visit VIDIZMO Data Processing Agreement.

3. INCIDENT RESPONSE AND RISK MANAGEMENT

3.1. Incident Response and Remediation

VIDIZMO maintains a documented Incident Response Plan to rapidly handle any Security Incident involving Customer Personal Data. The steps are as follows:

- Detect & Triage – Continuous monitoring triggers immediate escalation to the incident team.
- Contain & Mitigate – Isolate affected systems and apply short-term controls to limit impact.
- Investigate & Assess – Determine root cause, scope, data elements affected, and risk.
- Remediate & Recover – Eliminate vulnerabilities, rotate credentials if needed, restore services, and harden controls to prevent recurrence.
- Document & Review – Record all actions and evidence; conduct a post-incident review to improve procedures and safeguards.

3.2. Breach Notification and Regulatory Cooperation

If VIDIZMO confirms a Customer Data Breach, we will notify the Controller or primary Processor without undue delay and no later than 2 business days after confirmation (or sooner if required by law/contract).

3.2.1. Content of the notice

- Description of the breach, including categories and approximate numbers of data subjects and records affected.
- Likely consequences.
- Measures taken or proposed to address and mitigate the breach.

If full details are not yet known, an initial notice will be sent, followed by timely updates as facts are established.

3.2.2. Responsibilities

- Where attributable to VIDIZMO's acts or omissions, investigation and remediation are performed at VIDIZMO's expense.

- VIDIZMO will reasonably assist the Controller/primary Processor with regulatory notifications and communications to affected data subjects.
- All breach-related actions, evidence, and communications are logged and retained to demonstrate compliance.

3.3. Vulnerability Management and Penetration Testing

VIDIZMO conducts automated vulnerability scans weekly across applications, APIs, and cloud resources to identify and address security risks. Scans use up-to-date signatures and, where appropriate, authenticated checks to improve coverage. Findings are triaged and prioritized by severity, exploitability, and business impact, then tracked to closure with time-bound remediation targets and verification testing.

In addition, biannual penetration tests (VAPT) are performed by independent assessors to evaluate the platform's resilience against real-world attack techniques. Tests cover application and network layers and include retesting to confirm that remediation is effective.

These activities are part of a continuous risk-management cycle—detect → assess → remediate → verify → learn—with results reviewed by security leadership, integrated into our SDLC, and retained as evidence for audits and compliance.

3.4. Risk Management

VIDIZMO maintains an enterprise risk management process. Risks are identified through vulnerability scans, penetration tests, audits, vendor reviews, change reviews, and incidents. Each item is logged in a risk register, assessed for likelihood and impact, assigned an owner, and tracked in a ticketing system with due dates. Residual-risk decisions are documented at the appropriate management level. Periodic summaries go to security and product leadership.