VIDIZMO.AI

TRUST CENTER

Security & Compliance

A complete reference to VIDIZMO's security, privacy, and compliance program.

Every certification, technical standard, and regulatory compliance VIDIZMO supports: what each one requires, and exactly how VIDIZMO meets it.

Last Updated July 2026

ABOUT THIS WHITEPAPER

How to use this document

WHAT THIS DOCUMENT IS

This whitepaper is the complete written record of VIDIZMO's Trust Center: every certification, technical standard, and regulatory compliance VIDIZMO supports, what each one actually requires, and exactly how VIDIZMO meets that requirement. It also covers the core security practices that run underneath all of it (encryption, access control, incident response, data residency, and business continuity), and how responsibility is split between VIDIZMO and the customer in a SaaS deployment.

WHY IT EXISTS

This document exists to give one accurate, unambiguous account of VIDIZMO's security and compliance posture, so that account teams, compliance reviewers, auditors, and customers are all working from the same information instead of each side reconstructing it differently. It states plainly what VIDIZMO holds directly, what is inherited through infrastructure such as Microsoft Azure, and what is not currently documented, so nothing is left ambiguous.

WHO THIS IS FOR

This document is written for IT security teams, compliance officers, legal reviewers, and account teams who need a direct, reliable reference on VIDIZMO's security and compliance posture, rather than reconstructing the answer from memory or scattered sources each time it comes up.

Contents

From the program at a glance to the practices behind every control.

Trust Program Practices 25

Security, Privacy, and Compliance You Can Verify

VIDIZMO runs one Information Security and Product Security program across its entire platform. The job is straightforward: protect customer data, keep the service available, and keep it accurate.

CERTIFICATIONS, STANDARDS, AND COMPLIANCE

Certifications

ISO/IEC 27001:2022 · SOC 2 Type II · CSA STAR · FedRAMP High · PCI DSS

Standards

CJIS Security Policy · NIST 800-53 · FIPS 140-3 · WCAG 2.2 AA & Section 508 · NIST AI RMF

Compliance

HIPAA · GDPR / CCPA-CPRA

The VIDIZMO Trust Program

Data Protection & Encryption

- AES-256 encryption at rest
- TLS 1.2 minimum in transit (TLS 1.3 supported)
- Separate encryption keys per tenant, managed in Azure Key Vault and rotated biennially
- FIPS-compliant, NIST-recommended cryptography

Access Control & Identity

- SSO, MFA, and role-based access control (least privilege)
- Zero-standing-access for VIDIZMO staff: break-glass only, time-bound, fully logged
- Tenant isolation at application, database, and storage levels
- Zero Trust architecture with geo- and IP-based restrictions

Incident Response & Vulnerability Management

- Weekly automated vulnerability scans across apps, APIs, and cloud resources
- Quarterly independent penetration testing with retesting
- Security patches applied within 5 business days of vendor release
- Breach notification within 2 business days of confirmation

Responsible AI & Data Governance

- Customer data is never used to train AI models without explicit written consent
- Published Responsible AI Policy covering fairness, accountability, and safety
- Model inventory ("bill of models") available under NDA
- NIST AI Risk Management Framework alignment

Data Residency & Deployment Options

- SaaS (shared or dedicated), on-premises, private cloud, hybrid, bring-your-own-cloud, and fully air-gapped deployment models
- Data residency options include U.S.-based data centers, Canadian data centers (dedicated SaaS), and the Europe region
- Customer-chosen geographic region available for dedicated SaaS deployments
- Air-gapped deployments run entirely on-premises with no external network access; no data leaves the environment

Business Continuity & Disaster Recovery

- Recovery Time Objective: 48 hours
- Recovery Point Objective: 24 hours
- Geo-redundant storage with automated cross-region failover
- Semi-annual disaster recovery testing

Who Owns What in a SaaS Deployment

Application/platform security, secure SDLC, tenant isolation	VIDIZMO
Uptime SLA, vulnerability scanning, penetration testing	VIDIZMO
Incident response, breach notification, encryption, secure deletion	VIDIZMO

Data classification, content and metadata quality	CUSTOMER
Retention policies and legal holds	CUSTOMER
User and role administration, SSO/MFA/IdP policy	CUSTOMER
Audit log review, export and eDiscovery	CUSTOMER

Customer is the data Controller; VIDIZMO is the Processor; Microsoft Azure is the infrastructure sub-processor.

Certifications

VIDIZMO maintains a robust compliance framework to ensure the highest standards of data security, privacy, and operational integrity. VIDIZMO regularly undergoes independent third-party audits to achieve and maintain the following industry-recognized certifications:

- **ISO/IEC 27001:2022**
- **SOC 2 Type II**
- **CSA STAR**
- **FedRAMP High**
- **PCI DSS**

CERTIFICATION VIDIZMO-OWNED

ISO/IEC 27001:2022

Independently held by VIDIZMO, audited and issued in VIDIZMO's own name.

WHAT IT IS

ISO/IEC 27001:2022 is an internationally recognized standard for information security management systems (ISMS), independently audited and certified.

WHAT IT MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

- **An Information Security Management System (ISMS) with a defined scope:** covers the information security management system for all VIDIZMO service lines.
- **Ongoing risk assessment and treatment, and documented policies:** backed by a formal Information Security Program with regular internal risk assessments and policy reviews.
- **A certification audit by an accredited certification body, repeated on a 3-year cycle with annual surveillance audits:** VIDIZMO holds Certificate #RA-2507091, issued by the United Kingdom Accreditation Service (UKAS), VIDIZMO's accredited certification body, on July 9, 2025, valid through July 8, 2028.

Customers can review VIDIZMO's compliance annually, through a meeting with our team, a completed audit questionnaire, or supporting documentation, generally under a mutual non-disclosure agreement when sensitive internal detail is involved.

HOW THE ISMS IS MAINTAINED ACROSS THE LIFECYCLE

ISO 27001 requires the ISMS to stay effective on an ongoing basis, not just at audit time. VIDIZMO builds this into its Secure Software Development Lifecycle (SDLC):

- **Software Development**
  - Security user stories built into the Agile process
  - A Definition of Done that includes security requirements
  - Threat modeling before code is written
  - Secure code reviews
  - Static Application Security Testing (SAST) integrated into the development environment
- **Production**
  - Dynamic and Interactive Application Security Testing (DAST, IAST) during the testing phase
  - Patch management for third-party releases
  - Security gates with dependency scanning built into CI/CD pipelines (Azure DevOps, GitHub Actions)
- **Operations**
  - Weekly automated vulnerability scans
  - Quarterly independent penetration testing
  - Real-time audit logging retained in tamper-evident, immutable storage
  - A documented incident response plan
  - Annual security awareness training for staff

CERTIFICATION VIA AZURE

SOC 2 Type II

Inherited through Microsoft Azure's own attestation, not held by VIDIZMO in its own name.

WHAT IT IS

SOC 2 Type II is an attestation, examined by an independent auditor, that an organization's security controls against the Trust Services Criteria operated effectively over a defined review period, not just at a single point in time.

WHAT IT MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

SOC 2 Type II is scored against the AICPA's Trust Services Criteria, five categories that make up the full framework:

- **Security** (the Common Criteria, required in every SOC 2 report): protection against unauthorized access, both physical and logical.
- **Availability:** the system is available for operation and use as committed or agreed.
- **Processing Integrity:** system processing is complete, valid, accurate, timely, and authorized.
- **Confidentiality:** information designated as confidential is protected as committed or agreed.
- **Privacy:** personal information is collected, used, retained, and disposed of in accordance with commitments.

An independent auditor examines these controls over a defined review period, not just a single point in time. VIDIZMO meets this through Microsoft Azure's own SOC 2 Type II attestation, since VIDIZMO's infrastructure runs on Azure.

CERTIFICATION VIA AZURE

CSA STAR

A cloud-specific security registration, inherited through Microsoft Azure the same way SOC 2 is.

WHAT IT IS

The Cloud Security Alliance's Security, Trust, Assurance, and Risk (STAR) program assesses cloud providers against the Cloud Controls Matrix (CCM), a security framework built specifically for cloud services.

WHAT IT MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

- **A cloud-specific security assessment against the Cloud Controls Matrix.** Inherited through Microsoft Azure's own CSA STAR registration, since VIDIZMO's infrastructure runs on Azure.

SCOPE & LIMITATIONS

VIDIZMO does not hold a CSA STAR registration independently. ISO 27001 is the certification VIDIZMO holds directly.

CERTIFICATION | TWO PATHS AVAILABLE

FedRAMP High

A concrete path to FedRAMP High for DEMS, with a real timeline, not a vague one.

WHAT IT IS

FedRAMP (Federal Risk and Authorization Management Program) is the U.S. government's standardized approach to security assessment and authorization for cloud products used by federal agencies. FedRAMP High is the highest impact-level authorization, required for the most sensitive federal workloads.

WHAT FEDRAMP HIGH MAJORLY REQUIRES

- **Full implementation of the NIST SP 800-53 High control baseline:** hundreds of security controls across access, audit, encryption, and incident response.
- **Continuous monitoring:** ongoing vulnerability scanning and reporting to the authorizing body, not a one-time assessment.
- **Independent assessment by a certified Third-Party Assessment Organization (3PAO).**
- **A named agency sponsor, or the FedRAMP Joint Authorization Board, to actually issue the Authorization to Operate (ATO).**

HOW VIDIZMO SUPPORTS IT

VIDIZMO does not hold an independent FedRAMP ATO. There are two paths to FedRAMP High coverage for a DEMS deployment:

- **Microsoft Azure Government Cloud:** if you already run, or want to self-host VIDIZMO in, your own Azure Government Cloud environment, that infrastructure is already FedRAMP High authorized. Extending that authorization to VIDIZMO's application layer still requires your agency to sponsor it.
- **ProjectHost-authorized environment:** covers both infrastructure and application-level authorization. Does not require agency sponsorship. Typically delivered in 3 to 4 months, at additional cost.

SCOPE & LIMITATIONS

Neither path means VIDIZMO independently holds a FedRAMP ATO. The Azure Government Cloud path requires an agency sponsor before VIDIZMO's application layer is covered; the ProjectHost path removes that dependency but adds cost and a 3 to 4 month timeline.

CERTIFICATION | NOT HELD BY VIDIZMO

PCI DSS

PCI DSS does not apply to VIDIZMO in its own right. We do not process, store, or transmit cardholder data or handle financial transactions as part of our business. Where it matters is on the customer's side: if you're a bank, payment processor, or any organization storing payment-related records, VIDIZMO can help you meet your own PCI DSS obligations for that data.

WHAT IT IS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements for organizations that handle cardholder data, covering how that data is stored, processed, and protected.

WHERE VIDIZMO FITS

VIDIZMO is not a payment processor and does not hold a PCI DSS Attestation of Compliance in its own name. Cardholder data is not something VIDIZMO deals in as part of its core business. Where this becomes relevant is Redactor: when a customer's documents, images, or recordings contain payment-related information, Redactor's existing platform controls can help that customer meet several PCI DSS requirements on their own systems.

WHAT PCI DSS MAJORLY REQUIRES, AND HOW REDACTOR HELPS

- **Protect cardholder data:** encryption at rest and in transit. Redactor runs on the same AES-256 at rest and TLS in transit as every other VIDIZMO product, and automates redaction of payment-related information from documents, images, video, and audio.
- **Implement strong access control:** role-based access on a need-to-know basis, unique user IDs, and MFA, so only authorized users can view unredacted content.
- **Maintain a vulnerability management program:** weekly automated vulnerability scans and quarterly independent penetration testing across the platform.
- **Regularly monitor and test networks:** real-time audit logging of every redaction action, retained in tamper-evident, immutable storage.

SCOPE & LIMITATIONS

This describes how Redactor's controls can support your own PCI DSS program; it is not a certification VIDIZMO holds. VIDIZMO does not determine or validate your PCI DSS scope, Self-Assessment Questionnaire type, or overall compliance status; contact VIDIZMO directly for that detail.

Standards

VIDIZMO aligns its platform, cryptography, and accessibility practices to the following published technical frameworks and standards:

- **CJIS Security Policy**
- **NIST 800-53**
- **FIPS 140-3**
- **WCAG 2.2 AA & Section 508**
- **NIST AI RMF**

STANDARD | SUPPORTED PLATFORM-WIDE

CJIS Security Policy

Supported across every VIDIZMO product and every deployment option, not just Azure Government Cloud.

WHAT IT IS

The FBI's Criminal Justice Information Services (CJIS) Security Policy sets the minimum security requirements for any organization that accesses, transmits, or stores Criminal Justice Information (CJI), including systems used by law enforcement, courts, and prosecution agencies.

WHAT CJIS MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

The CJIS Security Policy is organized into policy areas covering identity, encryption, auditing, incident response, and personnel. Here is how VIDIZMO's platform maps to the areas that come up most, across the entire platform, not limited to Azure Government Cloud:

- **Advanced authentication for anyone accessing Criminal Justice Information:** Single Sign-On and Multi-Factor Authentication are enforced on a least-privilege basis, with Role-Based Access Control limiting what each user can see.
- **Encryption of CJI at rest and in transit, using FIPS-validated cryptography:** AES-256 encryption at rest and TLS 1.2 minimum (1.3 supported) in transit, through FIPS-compliant cryptographic modules.

- **Audit logging of all access to CJI:** real-time audit logging of all activity, retained in tamper-evident, immutable storage.
- **Ongoing vulnerability management and incident response:** weekly automated vulnerability scans, quarterly independent penetration testing, and a documented incident response plan with breach notification within 2 business days of confirmation.
- **Secure sanitization of media and data at end of life:** VIDIZMO's platform runs on a configurable software lifecycle purge policy. The default retention period is 30 days, and customers can adjust it to their own requirements at any point. Once the retention window elapses, data is sanitized in line with NIST SP 800-88 and permanently deleted.

SCOPE & LIMITATIONS

CJIS also requires background checks for personnel with access to CJI, including hands-on delivery staff. VIDIZMO's standard delivery model is offshore-staffed; background-checked onshore personnel are available, but require advance planning and lead time to hire and onboard. If your organization needs infrastructure-level CJIS authorization, for example on Azure Government Cloud, confirm that against your exact deployment directly with VIDIZMO.

STANDARD | SUPPORTED ON AZURE GOVERNMENT CLOUD

NIST 800-53

The federal security control catalog VIDIZMO supports on Azure Government Cloud deployments.

WHAT IT IS

NIST Special Publication 800-53 is the federal catalog of security and privacy controls that federal information systems, and organizations handling federal or CJIS-scoped data, are required to implement. It covers control families including access control, audit and accountability, encryption, incident response, and configuration management.

HOW NIST 800-53 IS ORGANIZED

NIST SP 800-53 groups its controls into three broad types, based on how they reduce risk:

- **Management controls:** address risk through policy, planning, and oversight.
- **Operational controls:** address risk through people, processes, and day-to-day practices.
- **Technical controls:** address risk through technology enforced in systems and software.

Those control types are organized into 20 families in Revision 5:

AC	Access Control	**AT**	Awareness and Training
AU	Audit and Accountability	**CA**	Assessment, Authorization, and Monitoring
CM	Configuration Management	**CP**	Contingency Planning
IA	Identification and Authentication	**IR**	Incident Response
MA	Maintenance	**MP**	Media Protection
PE	Physical and Environmental Protection	**PL**	Planning
PM	Program Management	**PS**	Personnel Security
PT	PII Processing and Transparency	**RA**	Risk Assessment
SA	System and Services Acquisition	**SC**	System and Communications Protection
SI	System and Information Integrity	**SR**	Supply Chain Risk Management

PT and SR were added in Revision 5.

WHAT NIST 800-53 MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

VIDIZMO's platform maps most directly to four of the twenty families:

- **Access Control (AC):** least-privilege, role-based access enforced through Single Sign-On, Multi-Factor Authentication, and Role-Based Access Control. See Access Control & Identity for the full detail.
- **Audit and Accountability (AU):** real-time audit logging of all activity, retained in tamper-evident, immutable storage.
- **System and Communications Protection (SC):** encryption for data at rest and in transit, and key management, implemented through FIPS 140-3 validated cryptographic modules. See FIPS 140-3 for the full detail.
- **Incident Response (IR):** weekly automated vulnerability scans, quarterly independent penetration testing, and breach notification within 2 business days of confirmation.

VIDIZMO supports SP 800-53, SP 800-171, and SP 800-60 specifically on Azure Government Cloud deployments.

DEVELOPMENT, TESTING, AND EVALUATION (SA, CA)

NIST SP 800-53 also covers how systems are built, tested, and assessed, largely through the System and Services Acquisition (SA) and Assessment, Authorization, and Monitoring (CA) families. VIDIZMO builds this in from the start rather than treating it as a one-time check:

- **Development:** threat modeling to identify risks before code is written, and Static Application Security Testing (SAST) integrated into the development environment.
- **Testing:** Dynamic and Interactive Application Security Testing (DAST, IAST) during the testing phase, plus security gates and dependency scanning built into CI/CD pipelines (Azure DevOps, GitHub Actions).
- **Evaluation:** weekly automated vulnerability scans and quarterly independent penetration testing, monitoring the platform continuously rather than assessing it once.

SCOPE & LIMITATIONS

The mapping above covers 4 of the 20 NIST SP 800-53 families, the ones that come up most in evaluations, not the full catalog. VIDIZMO's SP 800-53, SP 800-171, and SP 800-60 support is specific to Azure Government Cloud deployments. On standard commercial Azure, VIDIZMO's platform controls align with many of the same control families, but this is not a substitute for a formal SP 800-53 control assessment or Authorization to Operate. Contact VIDIZMO directly to confirm formal scope against your exact deployment.

STANDARD | FIPS 140-3 VIA AZURE CRYPTOGRAPHIC MODULES

FIPS 140-3

How VIDIZMO encrypts data at rest and in transit, manages keys, and applies FIPS 140-3 validated cryptography.

WHAT IT IS

FIPS 140-3 is the current U.S. government standard for cryptographic modules, covering how they are designed, tested, and validated for handling sensitive data. It replaced FIPS 140-2 as the standard cryptographic modules are validated against.

HOW FIPS 140-3 IS ORGANIZED

FIPS 140-3 defines four increasing security levels for a cryptographic module, based on the physical and logical protections it has:

- **Level 1:** basic security requirements, no dedicated physical security mechanisms required.
- **Level 2:** adds tamper-evidence and role-based authentication.
- **Level 3:** adds tamper-detection and response, and identity-based authentication.
- **Level 4:** adds tamper-detection and response under fluctuating environmental conditions, the highest level of assurance.

WHAT FIPS 140-3 MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

- **Validated cryptographic modules** covering key generation, storage, and destruction, at a defined security level: VIDIZMO applies FIPS-compliant, NIST-recommended cryptography through Azure's certified cryptographic modules.
- **Use of NIST-approved algorithms only:** non-approved or legacy algorithms are not permitted inside the validated boundary. VIDIZMO's encryption stack uses NIST-approved algorithms exclusively, including AES-256 and TLS 1.2/1.3.

For how VIDIZMO applies encryption day to day, data at rest, data in transit, and key management, see Data Protection & Encryption.

SCOPE & LIMITATIONS

VIDIZMO supports FIPS 140-3 through Azure's cryptographic modules. Customer-managed encryption keys (bring-your-own-key) and third-party key management integration are not currently documented as supported configurations; contact VIDIZMO directly if this applies to your evaluation.

STANDARD COMPLIANCE

WCAG 2.2 AA & Section 508

The technical accessibility standard VIDIZMO supports across every product, and the federal regulation that requires it.

WHAT IT IS

The Web Content Accessibility Guidelines (WCAG) 2.2 AA is the technical standard that defines what makes web content usable by people with disabilities, covering things like keyboard navigation, screen reader compatibility, and color contrast. Section 508 of the Rehabilitation Act is the U.S. federal regulation that requires this: it is the law, and WCAG 2.2 AA is the technical standard federal agencies use to measure conformance against it.

WHAT WCAG 2.2 AA MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

WCAG is organized around four principles, sometimes shortened to POUR:

- **Perceivable:** text alternatives for non-text content, captions, and sufficient color contrast.
- **Operable:** full keyboard navigation, no content that triggers seizures, and enough time for users to read and interact.
- **Understandable:** readable, predictable interface behavior.
- **Robust:** compatible with assistive technology such as screen readers.

WCAG 2.2 AA conformance is supported across the entire VIDIZMO platform.

WHAT SECTION 508 MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

- **Federal agencies must procure Information and Communication Technology (ICT) that meets defined accessibility standards**, referencing WCAG success criteria as the technical measure of conformance.
- **Functional Performance Criteria for users with vision, hearing, or mobility limitations.**

Section 508 alignment is supported across the entire VIDIZMO platform, built on the same WCAG 2.2 AA conformance work above.

VPAT REPORT

A per-success-criterion conformance report (VPAT) documenting WCAG 2.2 AA and Section 508 conformance is available to download.

Download VPAT Report

STANDARD

NIST AI RMF

The voluntary federal framework for managing AI risk, and how VIDIZMO's practices map to it.

WHAT IT IS

The NIST AI Risk Management Framework (AI RMF) is a voluntary framework published by the National Institute of Standards and Technology to help organizations manage risks from artificial intelligence throughout its lifecycle. It is not a certification: there is no audit or attestation to hold, only a structure to align practices against.

THE SEVEN CHARACTERISTICS OF TRUSTWORTHY AI

NIST AI RMF defines trustworthy AI by seven characteristics. Here is what each means, and where VIDIZMO has concrete evidence behind it today:

- **Valid and reliable:** the system performs as intended, consistently, across the conditions it is meant to operate in.
- **Safe:** the system does not endanger human life, health, property, or the environment.
- **Secure and resilient:** the system withstands adverse events and keeps operating. VIDIZMO backs this with platform-wide encryption, access control, and incident response, the same practices covered elsewhere in this Trust Center.
- **Accountable and transparent:** the organization behind the system is answerable for how it is built and used. VIDIZMO's published Responsible AI Policy and model inventory, the "bill of models," provide that visibility.
- **Explainable and interpretable:** outputs can be understood in the context of the system's design and intended use.
- **Privacy-enhanced:** the system respects how data is collected, used, and retained. VIDIZMO does not train models on customer data without explicit written authorization.
- **Fair, with harmful bias managed:** the system avoids unjust or systematically unfavorable treatment of individuals or groups.

WHAT NIST AI RMF MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

NIST AI RMF is organized around four functions, each broken into more specific categories. They are meant to work together on an ongoing basis, not as a one-time checklist:

- **Govern:** builds a culture of AI risk management across the organization, and cuts across the other three functions rather than sitting apart from them.
  - Policies, processes, and practices for AI use, and how transparently they are enforced

  - Accountability structures: defined roles, responsibilities, and reporting lines for AI decisions
  - Documented organizational risk tolerance for AI use
  - Workforce culture: diversity, equity, and risk-awareness across the teams building and operating AI
  - Processes for managing third-party and supply chain AI risk

  VIDIZMO's published Responsible AI Policy sets that accountability structure, covering fairness, accountability, transparency, and safety.
- **Map:** establishes the context for a specific AI system before it is assessed further.
  - The context: what the system is intended to do, and the business purpose behind it
  - Who uses the system and how, including the specific use case it is deployed for
  - What could realistically go wrong for the people affected by that use case

  This is reflected in VIDIZMO's model inventory, the "bill of models," available under NDA.
- **Measure:** analyzes and monitors AI risk on an ongoing basis, not just at launch.
  - Quantitative methods: measurable metrics tested against defined risk thresholds
  - Qualitative methods: structured review and expert judgment where behavior is not easily reduced to a number
  - Tracking identified risks over time, not just at a single point of testing

  VIDIZMO applies the same secure development lifecycle to AI features as the rest of the platform: threat modeling, static and dynamic application security testing, and independent penetration testing.
- **Manage:** allocates resources to the risks identified through Map and Measure.
  - Deciding whether to mitigate, transfer, avoid, or accept each identified risk
  - Planning and implementing responses that maximize benefit and minimize harm
  - Monitoring risk treatments after deployment, not only before launch

  VIDIZMO does not train models on customer data by default, only with explicit written authorization, and AI-driven features are covered by the same incident response process as the rest of the platform.

SCOPE & LIMITATIONS

NIST AI RMF is voluntary: there is no certification or independent audit to hold against it. What is described above is how VIDIZMO's existing practices map to the framework's structure, not a formal attestation. VIDIZMO's documented evidence maps most directly to the secure and resilient, accountable and transparent, and privacy-enhanced characteristics. Contact VIDIZMO directly if you need evidence against a specific characteristic or function.

Compliance

VIDIZMO supports the following regulatory and legal frameworks so customers can meet their own compliance obligations:

- **HIPAA**
- **GDPR & CCPA-CPRA**

COMPLIANCE

HIPAA

VIDIZMO is not a healthcare provider. Many of our customers and use cases are in healthcare and need HIPAA compliance, and VIDIZMO provides the safeguards to get them there, across every product.

WHAT IT IS

The Health Insurance Portability and Accountability Act (HIPAA) sets requirements for protecting health information in the United States. It applies to healthcare providers, health plans, and their business associates, organizations that handle protected health information (PHI) on a covered entity's behalf.

WHERE VIDIZMO FITS

VIDIZMO is not a healthcare provider, health plan, or insurer, and does not bill for medical services. Our customers and use cases very much are in healthcare: agencies and organizations across DEMS, EnterpriseTube, and Redactor regularly handle health-related records, from medical evidence to patient video and audio. When a customer stores or processes PHI on the platform, VIDIZMO functions as that customer's business associate under HIPAA, and helps them meet their HIPAA compliance obligations through the technical, administrative, and physical safeguards described below.

WHAT HIPAA MAJORLY REQUIRES, AND HOW VIDIZMO SUPPORTS IT

- **Technical safeguards** (access control, audit controls, integrity, and transmission security): SSO, MFA, and role-based access control on a least-privilege basis; AES-256 encryption at rest and TLS in transit; real-time audit logging retained in tamper-evident, immutable storage.

- **Administrative safeguards** (risk analysis and workforce training): covered by VIDIZMO's Information Security Program, including onboarding and annual security awareness training for staff.
- **Physical safeguards** (facility and workstation security): handled at the Microsoft Azure data center level.
- **Breach Notification Rule** (notify affected parties without unreasonable delay): VIDIZMO commits to notification within 2 business days of confirmation.

SCOPE & LIMITATIONS

Whether VIDIZMO will execute a Business Associate Agreement (BAA), and any related pricing impact, is not documented on this page. Confirm this directly with your account team rather than assuming either way.

COMPLIANCE

GDPR & CCPA-CPRA

How VIDIZMO supports EU data protection and California consumer privacy requirements.

WHAT IT IS

The General Data Protection Regulation (GDPR) governs data protection and privacy in the EU. The California Consumer Privacy Act and its successor, the CPRA, do the same for California residents. Both give individuals rights over their personal data and place obligations on the organizations that process it.

WHAT THEY MAJORLY REQUIRE, AND HOW VIDIZMO SUPPORTS THEM

- **A lawful basis for processing and a data processing agreement between controller and processor:** a Data Processing Agreement (DPA) is available, naming VIDIZMO as Processor and the customer as Controller.
- **Security of processing (GDPR Article 32):** AES-256 encryption at rest, TLS in transit, and role-based access control.
- **Breach notification to the supervisory authority within 72 hours (GDPR):** VIDIZMO commits to notifying the customer within 2 business days of confirmation, ahead of that window, so the customer can meet its own regulatory deadline.
- **Support for Data Protection Impact Assessments (DPIAs) on high-risk processing:** VIDIZMO cooperates in good faith with audits and provides reasonable DPIA support.
- **Data residency for EU personal data:** supported through the Europe region, in two ways.
  - **Local deployment in Europe:** VIDIZMO can be deployed on the customer's own infrastructure, physically located in Europe.
  - **SaaS with a European-region Azure Blob:** the SaaS itself is still VIDIZMO-hosted, but the underlying Azure Blob Storage can be set to a customer-chosen European region, so data at rest stays there.

  For AI-driven processing, such as redaction, transcription, or search, data moves temporarily into VIDIZMO's processing systems and is deleted immediately once processing completes. This handling is governed under the Data Processing Agreement.
- **Consumer rights to know, delete, and opt out of sale (CCPA/CPRA):** supported through the same access-control and data-handling practices applied platform-wide.

Trust Program Practices

The certifications and standards above are backed by the following operating practices, run continuously across the platform:

- **Data Protection & Encryption**
- **Access Control & Identity**
- **Incident Response & Vulnerability Management**
- **Data Residency & Deployment Options**
- **Business Continuity & Disaster Recovery**

STANDARD

Data Protection & Encryption

How VIDIZMO protects data at rest and in transit, and manages encryption keys across the platform.

WHAT IT IS

Data protection and encryption cover how information is secured while it is stored and while it moves across the platform, and how the encryption keys that protect it are generated, stored, and rotated.

HOW VIDIZMO IMPLEMENTS IT

- **Data at rest:** AES-256 encryption.
- **Data in transit:** TLS 1.2 minimum, TLS 1.3 supported.
- **Key management:** Azure Key Vault, with separate encryption keys per tenant, rotated biennially.
- **Cryptography:** FIPS-compliant, NIST-recommended algorithms, validated under FIPS 140-3. See FIPS 140-3 for the full standard detail.

MALWARE DETECTION

- Ingestion-time malware scanning on all uploaded content
- Infected files quarantined automatically; not accessible until reviewed
- Admin review workflow: quarantined files can be released or permanently deleted by administrators

- Applies to all file uploads across every product (DEMS, EnterpriseTube, AI Intelligence Hub, Redactor, AI Live Insight)

SCOPE & LIMITATIONS

Customer-managed encryption keys (bring-your-own-key) and third-party key management integration are not currently documented as supported configurations; contact VIDIZMO directly if this applies to your evaluation.

STANDARD

Access Control & Identity

Who can get in, what they can see, and how VIDIZMO keeps its own staff out of your data by default.

WHAT IT IS

Access control and identity management cover how a system verifies who a user is and limits what they can do once they're in. For a platform holding evidence, video, and sensitive records, this is usually the first thing a security reviewer checks.

HOW VIDIZMO IMPLEMENTS IT

- Single Sign-On, Multi-Factor Authentication, and Role-Based Access Control, provisioned on a least-privilege, need-to-know basis
- Phish-resistant MFA through the customer's own identity provider, including FIDO2/WebAuthn security keys and smartcards via Microsoft Entra ID
- SCIM provisioning for automated user onboarding and offboarding
- Zero Trust architecture, with geo-restriction and IP allow/deny lists at the tenant and per-content level
- Tenant isolation enforced at the application, database, and storage layers
- All activity logged and monitored for suspicious behavior, with audit trails retained for compliance

VIDIZMO STAFF ACCESS

VIDIZMO staff do not hold standing access to customer data. Access is granted only through a break-glass process: time-bound, requiring MFA, and fully logged for review.

STANDARD

Incident Response & Vulnerability Management

What happens when something goes wrong, and how VIDIZMO looks for problems before they do.

INCIDENT RESPONSE PLAN

VIDIZMO follows a documented five-step process for any security incident involving customer data:

- **Detect & Triage:** continuous monitoring triggers immediate escalation
- **Contain & Mitigate:** isolate affected systems and apply short-term controls
- **Investigate & Assess:** determine root cause, scope, and risk
- **Remediate & Recover:** eliminate the vulnerability, rotate credentials if needed, restore service
- **Document & Review:** record every action and run a post-incident review

BREACH NOTIFICATION

If VIDIZMO confirms a breach involving customer data, the customer's Controller or primary Processor is notified within 2 business days of confirmation, sooner if law or contract requires it. The notice covers what happened, who and what was affected, and what VIDIZMO is doing about it.

VULNERABILITY MANAGEMENT & PENETRATION TESTING

- Weekly automated vulnerability scans across applications, APIs, and cloud resources
- Findings triaged by severity, exploitability, and business impact, then tracked to closure with verification testing
- Security patches applied within 5 business days of vendor release; emergency hotfixes deployed immediately
- Quarterly penetration testing (VAPT) by independent assessors, covering application and network layers, with retesting to confirm fixes hold

BUILT INTO DEVELOPMENT

Threat modeling happens during development, not after. Static, dynamic, and interactive application security testing (SAST, DAST, IAST) run through the sprint cycle, and patch management tracks third-party vendor releases so known vulnerabilities don't sit unaddressed.

STANDARD

Data Residency & Deployment Options

Where data lives, and how VIDIZMO can be deployed, from shared SaaS to fully air-gapped, on-premises environments.

DEPLOYMENT MODELS

- **SaaS (shared):** multi-tenant, VIDIZMO-managed, most cost-effective, self-service in about 30 seconds
- **SaaS (dedicated):** single-tenant infrastructure for stricter security and performance requirements
- **On-Premises:** installed on the customer's own servers; full control, customer owns disaster recovery and maintenance
- **Private Cloud:** hosted in the customer's own cloud (Azure, AWS, etc.), dedicated and customer-controlled
- **Hybrid:** sensitive workloads on-premises, burstable workloads in the cloud
- **Bring Your Own Cloud (BYOC):** deployed in the customer's cloud environment, with VIDIZMO managing the application layer
- **Air-Gapped:** fully disconnected, no external network access, all AI processing runs locally; built for defense, intelligence, and classified environments

DATA RESIDENCY

- U.S.-based data centers, including Azure Government and AWS GovCloud
- Canadian data centers available for dedicated SaaS deployments
- **Europe region:** supported in two ways.
  - **Local deployment in Europe:** VIDIZMO can be deployed on the customer's own infrastructure, physically located in Europe.
  - **SaaS with a European-region Azure Blob:** the SaaS itself is still VIDIZMO-hosted, but the underlying Azure Blob Storage can be set to a customer-chosen European region, so data at rest stays there.

  For AI-driven processing, such as redaction, transcription, or search, data moves temporarily into VIDIZMO's processing systems and is deleted immediately once processing completes. This handling is governed under the Data Processing Agreement.
- Customer-chosen geographic region available for dedicated SaaS deployments

CLOUD PLATFORMS

VIDIZMO is cloud-agnostic at the infrastructure level. Microsoft Azure is the primary platform where PaaS services (Cognitive Services, Azure OpenAI, Media Services) are actively used; AWS, Google Cloud, and Oracle Cloud are supported at the VM/container infrastructure level.

STANDARD

Business Continuity & Disaster Recovery

How VIDIZMO keeps the platform running, and recovers quickly when something fails.

RECOVERY OBJECTIVES

- **Recovery Time Objective (RTO):** 48 hours
- **Recovery Point Objective (RPO):** 24 hours

ARCHITECTURE

- Azure Site Recovery for failover, Azure Traffic Manager for DNS-based routing
- Geo-Redundant Storage (3 primary and 3 secondary storage servers), with Zone-Redundant Storage available as an alternative
- Auto-scaling via Azure Virtual Machine Scale Sets
- Automated backup of VOD content, with optional daily backups retained for 30 days
- Data replicated across multiple Azure regions, with VMs physically separated across geo-redundant zones

TESTING & AVAILABILITY

- Semi-annual disaster recovery testing
- 99.9% uptime SLA, measured monthly
- Scheduled maintenance requires 48-hour advance notice and runs during non-peak hours; designed to never impact video playback

SCOPE & LIMITATIONS

For on-premises deployments, disaster recovery and backup are the customer's responsibility. VIDIZMO provides guidance on redundant hardware, failover, and SQL Server clustering, but does not operate DR for on-premises environments.