Douglass Brown

Arlecia Tyus

Security Policies & Procedures

May 10, 2026

Security Policy for enVisiAIn

Acceptable Use, Risk Assessment, and Remote Access

Introduction

enVisiAIn is a fictitious health technology company that creates AI-augmented vision tools for blind and low-vision users, elderly individuals, and rehabilitation clinics. The company's main products include smart glasses, a phone application, and a clinical dashboard. The smart glasses use computer vision, biometric sensors, and AI assistance to help users identify objects, read signs, detect hazards, recognize approved contacts, and navigate physical spaces. The mobile app allows users and caregivers to manage account settings, alerts, and permissions. The clinical dashboard allows rehabilitation clinics and authorized staff to monitor patient progress, review device performance, and support care.

Because enVisiAIn works in the health field, it collects and processes highly sensitive data. This may include live camera feeds, retinal scans, biometric readings from sensors inside the glasses, GPS location, medical history, insurance information, emergency contacts, voice commands, clinician notes, and AI-generated recommendations. The company attempts to keep as much data as possible on the device, while anonymizing or de-identifying data before it is used in cloud systems for analytics, research, or AI improvement.

This security policy focuses on three important areas: the Acceptable-Use Policy, Risk Assessment Policy, and Remote Access Policy. These policies are necessary because enVisiAIn's technology does not only affect business operations; it also affects patient privacy, safety, and trust. A data breach involving medical records, biometric data, live video, or location information could cause serious harm to users and damage the company's reputation.

Acceptable-Use Policy

Purpose

The purpose of the Acceptable-Use Policy is to define how employees, contractors, clinicians, vendors, and partners may use enVisiAIn systems. This policy applies to company laptops, mobile devices, smart glasses prototypes, internal networks, cloud systems, email, messaging platforms, source code repositories, patient records, clinical dashboards, and AI development environments.

An Acceptable-Use Policy is important because many security problems are caused by human behavior. Even if a company has strong technical controls, employees can still create risk by using weak passwords, downloading unauthorized software, sharing data improperly, or accessing information they do not need for their job. For enVisiAIn, this risk is especially serious because employees may handle medical records, biometric data, visual recordings, AI outputs, and patient location data.

Policy Requirements

All users must use enVisiAIn systems only for approved business, clinical, support, research, or operational purposes. Limited personal use may be allowed if it does not interfere with work, violate policy, or expose company systems to risk. Company systems may not be used for illegal activity, harassment, unauthorized surveillance, personal business, gambling, cryptocurrency mining, or accessing malicious content.

Employees and authorized users must protect company data at all times. Patient records, biometric readings, eye scans, live or stored video, location records, AI model data, source code, and internal research must not be copied, emailed, downloaded, photographed, uploaded, or shared outside approved systems. Users may not store company data in personal email accounts, personal cloud storage, unauthorized AI chatbots, personal messaging apps, or removable drives unless specifically approved.

All users must follow identity and access rules. Passwords, authentication tokens, MFA prompts, access badges, and login sessions may not be shared. Employees must lock their screens when away from their computers and must immediately report lost or stolen devices. Users may not attempt to access patient records, dashboards, code repositories, or databases outside their assigned job responsibilities.

Because enVisiAIn uses AI and computer vision, employees must follow special rules for AI data. Raw patient video, biometric data, retinal scans, and location data may not be used for AI training or testing unless approved by the security, privacy, and compliance teams. Whenever possible, AI development should use anonymized or de-identified data.

Rationale

This policy is necessary because enVisiAIn handles data that is more sensitive than ordinary business information. A careless employee action could expose where users live, what they see, what medical conditions they have, or how they move through the world. The Acceptable-Use Policy helps reduce insider misuse, accidental data exposure, malware infections, privacy violations, and unsafe AI data handling.

Risk Assessment Policy

Purpose

The purpose of the Risk Assessment Policy is to define how enVisiAIn identifies, evaluates, prioritizes, and responds to cybersecurity and privacy risks. A risk assessment policy is important because it helps the company find problems before they become major incidents. Without regular risk assessments, enVisiAIn could overlook threats involving smart glasses, mobile apps, cloud systems, clinical dashboards, AI models, vendors, and patient data.

For enVisiAIn, risk assessment must cover more than traditional computers and networks. The company must also assess risks involving wearable devices, biometric sensors, mobile applications, AI training pipelines, cloud storage, APIs, clinical workflows, emergency alerts, and third-party partners.

Policy Requirements

enVisiAIn must conduct a formal risk assessment at least once per year and whenever a major change occurs. Major changes include releasing a new smart glasses model, adding a new biometric sensor, launching a new AI feature, integrating with a new clinic, changing cloud providers, or allowing a new vendor to access sensitive systems.

Each risk assessment must identify important assets, possible threats, vulnerabilities, likelihood, impact, existing controls, missing controls, risk owners, recommended fixes, and target completion dates. Important assets include patient records, live video, stored video, retinal scans, biometric data, GPS location, clinician notes, AI models, source code, firmware, dashboard accounts, encryption keys, and cloud databases.

Risks should be classified as Low, Medium, High, or Critical. A Low risk has limited impact and does not involve sensitive data. A Medium risk may affect internal systems or business operations. A High risk may expose sensitive company, clinical, or patient data. A Critical risk may cause a major data breach, patient safety issue, ransomware incident, regulatory violation, or compromise of systems used for real-world navigation.

Any risk involving unauthorized access to live video, biometric data, medical records, location data, emergency alerts, production AI systems, or smart glasses firmware should be treated as High or Critical unless formally downgraded by security leadership.

enVisiAIn must also assess third-party risk. Since the company works with hospitals, rehabilitation clinics, universities, cloud providers, AI vendors, insurers, device manufacturers, and emergency-response partners, vendor security is a major concern. Vendors must be reviewed before receiving access to enVisiAIn systems or sensitive data. They must follow contract requirements for data protection, breach notification, encryption, retention, and approved use of company data.

Rationale

The Risk Assessment Policy is necessary because enVisiAIn operates in a complex environment where technology, healthcare, AI, and patient safety overlap. A weakness in the phone app could expose user location. A weakness in the dashboard could expose medical records. A weakness in smart glasses firmware could affect the user's ability to navigate safely. A weakness in a vendor's system could still harm enVisiAIn users.

This policy helps the company make security decisions based on actual risk instead of assumptions. It also helps leadership decide where to spend money, which systems need urgent protection, and which business processes need stronger controls.

Remote Access Policy

Purpose

The purpose of the Remote Access Policy is to define how employees, contractors, clinicians, vendors, and partners may access enVisiAIn systems from outside company-controlled locations. enVisiAIn is mostly an on-site company, but some employees work hybrid schedules. Certain engineers, executives, clinical support workers, vendors, and emergency-support staff may need remote access to company systems.

Remote access is useful, but it also creates serious risk. Employees may connect from home networks, hotels, clinics, public Wi-Fi, or other environments that enVisiAIn does not control. If remote access is not secured, attackers could steal credentials, access patient data, compromise dashboards, disrupt cloud systems, or interfere with company operations.

Policy Requirements

Remote access must be approved by management and the security team. Access must be based on job responsibility and the principle of least privilege. Users should only receive the access needed to perform their work.

All remote access must use company-approved secure tools such as VPN, zero-trust network access, secure cloud identity controls, or managed virtual desktops. Multifactor authentication is required for all remote access. Password-only remote access is prohibited. Remote sessions must be logged and may be monitored or reviewed.

Employees must use company-managed devices when accessing restricted systems. These devices must include endpoint protection, disk encryption, automatic updates, screen lock, device inventory tracking, and remote wipe capability. Personal devices may not be used to access patient records, biometric data, smart glasses telemetry, clinical dashboards, production cloud systems, or AI training data unless a formal exception is approved.

Users may not save company data to personal devices, personal cloud accounts, or removable drives. They may not print patient records at home or in public locations unless approved. They may not allow family members, friends, or unauthorized people to view company systems. Users may not use unauthorized remote desktop tools or disable security software.

Vendor remote access must be limited, monitored, and time-based. Vendors may only receive access when there is a documented business need, a signed agreement, an enVisiAIn sponsor, and security approval. Vendor access must be removed when the work is complete or when the relationship ends.

Emergency remote access may be allowed when necessary to restore service, investigate an outage, or protect patient safety. However, emergency access must still be logged, reviewed, and limited to the minimum access needed.

Rationale

The Remote Access Policy is necessary because remote access expands the company's attack surface. Attackers do not need to physically enter an enVisiAIn office if they can steal a remote worker's credentials or compromise an unmanaged device. For enVisiAIn, this risk is especially serious because remote systems may contain patient data, live support tools, AI systems, or smart glasses information.

This policy helps protect users by requiring strong authentication, approved devices, secure connections, logging, and limited access. It also supports hybrid work without allowing convenience to override patient privacy and system security.

Relationship Between the Three Policies

The Acceptable-Use Policy, Risk Assessment Policy, and Remote Access Policy work together to support enVisiAIn's overall security program.

The Acceptable-Use Policy focuses on behavior. It tells employees and partners how they are expected to use company systems, devices, applications, data, and AI tools. This reduces careless actions, misuse, and unauthorized data sharing.

The Risk Assessment Policy focuses on decision-making. It gives the company a process for identifying threats, ranking risks, and deciding what controls are needed. This helps enVisiAIn prioritize the most serious risks, especially those involving patient data, biometric information, AI systems, and wearable devices.

The Remote Access Policy focuses on access from outside company-controlled environments. It protects the company from risks created by hybrid work, vendors, home networks, public Wi-Fi, and unmanaged devices.

Together, these policies help enVisiAIn protect sensitive data and maintain trust. The company's mission depends on users feeling safe with technology that can see their surroundings, understand their movements, and support their care. If the company fails to protect that data, it could harm users and lose credibility.

Conclusion

enVisiAIn's products could improve the lives of blind and low-vision users, elderly individuals, and rehabilitation patients. However, the same technology that makes the company valuable also creates serious security responsibilities. The company handles medical records, biometric data, video, location information, voice commands, AI recommendations, and clinical support data. This makes cybersecurity central to the company's mission.

The Acceptable-Use Policy establishes clear rules for responsible system use. The Risk Assessment Policy gives the company a structured way to identify and manage threats. The Remote Access Policy protects systems when employees, vendors, and partners connect from outside company facilities. Each policy serves a different purpose, but together they help protect patients, employees, partners, and the business itself.

For enVisiAIn, security is not just a technical requirement. It is part of patient care. The company's users depend on its systems to safely understand and navigate the world. Because of that, protecting data, devices, access, and AI systems must be treated as a core business responsibility.

References

SANS Institute. "Security Policy Templates." SANS Institute.
U.S. Department of Health and Human Services. "Summary of the HIPAA Security Rule." HHS.gov.
European Union. "General Data Protection Regulation." EUR-Lex.