HTC SECURITY AND PRIVACY WHITEPAPER

April 2026

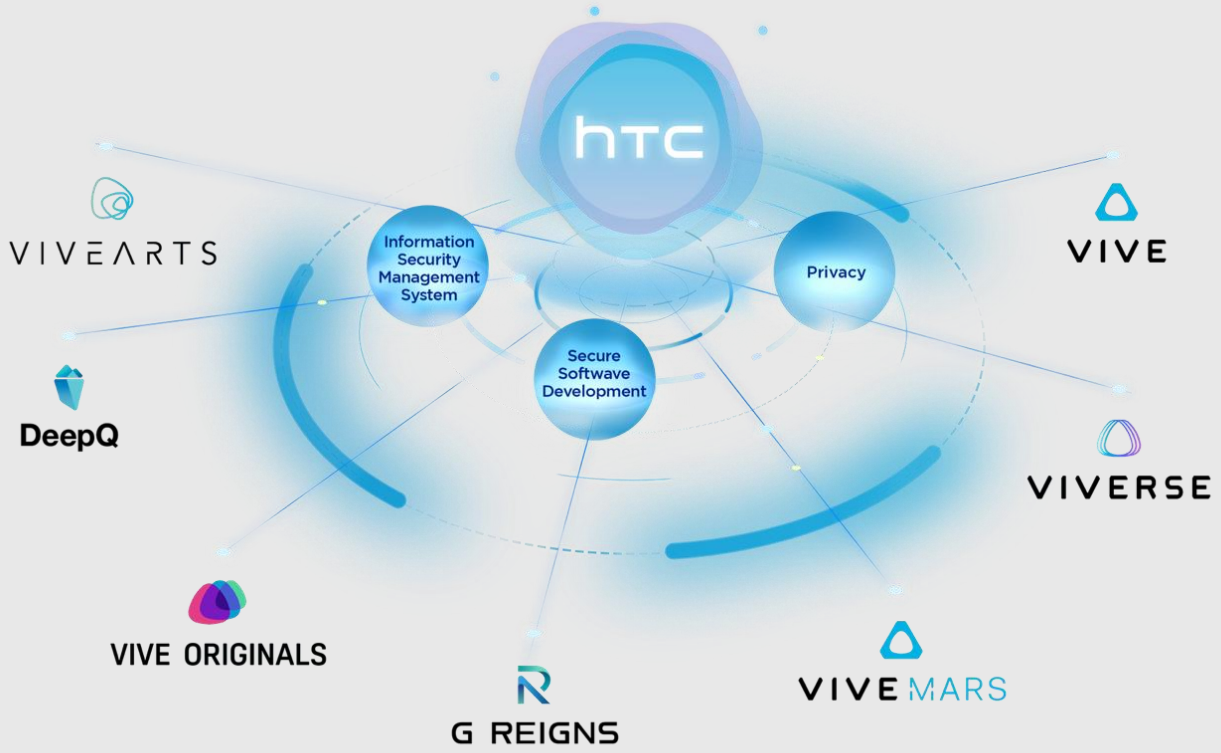
htc

VIVE

Content

Introduction

At HTC, we put people first. Whether you're an individual exploring immersive digital experiences or a business building innovative solutions, your trust is at the heart of everything we do. We believe that protecting your privacy and ensuring data security should never be an afterthought or sidetracked by competing priorities. Instead, privacy and security are our number-one focus, engineered into our products and services from the very start without ever resorting to data practices driven by advertising or social media imperatives.



Our approach combines advanced security technologies, proactive threat management, and strict compliance with international standards and regulations. By embedding security-by-design and privacy-by-design principles throughout every stage of development and operation, we create environments where security is seamless, transparency is standard, and individuals remain in control of their data. Whether you're a consumer or an enterprise partner, you can count on HTC to safeguard your information securely and privately.

Our Security and Privacy Principles

HTC's strategy is grounded in four core principles designed to safeguard both users and businesses:

Put People First

We prioritize the protection of user privacy and data security, ensuring that your personal and business information remains protected.

Trust through Transparency

We clearly communicate how data is managed, used, and protected.

Meaningful User Control

We embed practical, easy-to-use privacy and security controls into our products, giving you the power to manage your information confidently.

Continuous Improvement

We continuously enhance our security and privacy practices to address evolving threats and align with international best practices.

Comprehensive Security Measures

HTC implements a multi-layered security approach to protect your data, our products, and services.

Identity and Access Management (IAM)

We ensure only authorized users can access sensitive information:

- **Single Sign-On (SSO)**: One secure login for multiple HTC services.
- **Multi-factor Authentication (MFA)**: Adds extra layers of identity verification.
- **Role-based Access Control (RBAC)**: Access granted strictly based on role and necessity.

Device and Network Security

Your connection and devices are protected at every level:

- **Advanced Malware Detection**: Proactively identifies and blocks malicious software.
- **Vulnerability Scanning**: Regular checks to identify and fix potential weaknesses.
- **Real-time Threat Monitoring**: Continuous oversight to detect and respond to threats as they happen.

Physical Security Controls

We protect the physical spaces where your data might reside:

- **Controlled Access**: Only authorized personnel can enter sensitive areas.
- **24/7 Video Monitoring**: Ensures constant surveillance of key locations.
- **Detailed Access Logs**: Tracks all entries and exits to critical spaces.

Application and Data Security

Your data stays protected across all HTC services:

- **Secure Development Lifecycle (SDL)**: Security is built into every step of our product development process, from design to release.
- **Frequent Security Testing**: Regular testing by security experts to identify and fix vulnerabilities.
- **Encryption (at rest and in transit)**: Your data is always encrypted whether it's being stored or sent.

Privacy in HTC Products

Unlike many social media companies that build their business models around harvesting and monetizing personal data for targeted advertising, engagement metrics, or third-party profiling, HTC's sole focus is on delivering immersive and secure experiences. We have no hidden agendas, no advertising imperatives, and no data-driven motivations beyond making our products work better for you.

This unwavering commitment to "**privacy first, from design to delivery**" is what sets HTC apart. We design our products with strong, built-in privacy protections to ensure that your data remains truly yours.

Local Data Processing

Whenever possible, your information stays on your device. By keeping processing local, we eliminate the need to transmit sensitive data to the cloud.

User Consent Features

We never collect sensitive personal data without your clear, informed consent. Every time we ask for sensitive personal data, you decide whether to share it.

Transparency and Minimal Collection

We are upfront about our data practices and only collect the bare minimum necessary to deliver the best experience.

No Data Monetization

Unlike social networks that track, profile, and sell your data, HTC doesn't use your personal information for advertising or share it with third parties for profit.

Privacy by Design from Design to Delivery

From initial concept and design through development, deployment, and ongoing updates, privacy is engineered into every phase. Proactive risk assessments, privacy-protective defaults, and regular audits ensure that your data remains secure and that privacy controls stay aligned with emerging standards.

Achievements in Security and Privacy

HTC adheres to globally recognized security and privacy certifications, demonstrating our commitment to the highest standards:

- **ISO/IEC 27001**: Information Security Management
- **ISO/IEC 27701**: Privacy Information Management
- **ISO 27799**: Health Information Security (specifically for healthcare solutions)

These certifications reflect our unwavering commitment to maintaining robust security and privacy protections. Certification coverage is carefully determined according to the product security and privacy requirements of our major activities.

We're proud to announce that many of our key products have been certified to meet international standards:

- HTC Account, VIVERSE Market (Marketplace), VIVERSE Create, VIVERSE Avatar, VIVERSE for Business, and VIVE AI are all ISO/IEC 27001 and ISO/IEC 27701 certified. HTC is dedicated to continuously strengthening the security and privacy of its products and services. As a result, the scope of annual validations may evolve and expand over time. For the most up-to-date details, please consult your designated HTC representative.
- In healthcare, DeepQ meets the highest standards in medical data security, with certifications in ISO/IEC 27001, ISO/IEC 27701, and ISO 27799.

Continuous Improvement and Contact Information

Security and privacy are never one-time efforts. HTC continuously monitors, evaluates, and improves its practices to stay ahead of evolving threats and to maintain compliance with the latest standards.

If you have any questions or would like to learn more about how we protect your data and privacy, feel free to contact our dedicated security and privacy team. We're here to ensure you can use HTC services with complete confidence.

- For more information about HTC Security: security@htc.com
- For more information about HTC Privacy: global-privacy@htc.com

HTC Information Security Management System

HTC has established a comprehensive and structured Information Security Management System (ISMS) in full compliance with the ISO/IEC 27001 international standard. This system covers organizational structure, personnel management, technical safeguards, and process controls, aiming to systematically manage risks, ensure the confidentiality, integrity, and availability of the company's information assets, while strengthening data protection mechanisms and enhancing overall information security governance effectiveness.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Information Security Policy

HTC has established an Information Security Policy that is regularly reviewed and updated to ensure compliance with regulatory requirements and industry best practices. The policy is communicated to all relevant personnel to ensure the implementation of security standards.

People Controls

- All employees are required to understand the HTC Information Security Policy and to sign a non-disclosure agreement (NDA) during onboarding.
- Clear disciplinary procedures are established and enforced in the event of information security policy violations.
- Secure offboarding and role change processes are in place, including revoking system access, recovering company assets, and ensuring continued adherence to security obligations.
- Contractors and temporary staff are held to the same information security requirements, including signing NDAs and receiving appropriate training.

Identity and Access Management

- Employees must use identifiable login credentials and perform two-factor authentication to access internal systems, significantly enhancing account security.
- Account access rights are regularly reviewed to ensure users are granted only the minimum necessary permissions based on their roles.
- HTC platforms widely implement Role-based Access Control (RBAC) to enforce fine-grained access control and limit sensitive data access to authorized users only.

Endpoint Security

- Employee computers are managed, monitored, and protected with antivirus, USB access control, and device encryption mechanisms in place to ensure endpoint security. Mobile Device Management (MDM) is implemented to enforce security policies and manage device compliance.
- Protection and monitoring mechanisms are implemented for sensitive data leakage prevention.
- An anti-malware solution is deployed across endpoints and servers to detect, prevent, and remove malicious software, ensuring real-time protection against threats such as viruses, ransomware, and spyware.

Physical Security

- All HTC employees and visitors are required to wear identification badges. Besides, access control systems protect office areas, server rooms, production lines, and other restricted areas, and thus, employees can only enter areas using their unique identification credentials.
- Surveillance systems are set up at the entrances/exits to protect HTC information assets and employee safety, and CCTV (closed-circuit television) monitoring systems are also installed within secure areas.
- Regularly perform physical asset inventory, visitor management records, access control audits, and enhanced protection measures in controlled areas.

Network Security

- Data transmission for HTC products and services is transferred through secure encrypted channels.
- Servers and networks are protected by firewalls, Intrusion Prevention and Detection Systems (IPS/IDS), and Web Application Firewalls (WAF) and combine Distributed Denial of Service (DDoS) prevention mechanisms to properly safeguard.
- HTC company networks are subject to strict restrictions, segmentation, and layered protection, and includes VPN security channels, zero-trust architecture introduction, and network traffic anomaly detection and response processes.
- URL reputation filtering and malicious link blocking mechanisms are in place to prevent users from accessing phishing websites or other high-risk content.

Privacy Protection and Information Security Training

- HTC's new employee orientation includes privacy protection and company information protection training.
- HTC employees are required to complete annual privacy protection and information security training and exams to ensure training effectiveness.
- HTC employees involved in software product planning, development, testing, system management, operations, and vendor management must also complete courses and pass exams for "Product Software Security Process" and "Information Protection Guidelines."
- Personnel responsible for software product development must also complete training courses and exams on “Security by Design and by Default,” “Threat Model Analysis,” and “Secure Coding Standards for Key Programming Languages.”
- HTC's Privacy and Security team sends all HTC employees a monthly Privacy and Information Security newsletter to provide awareness promotion, real-time privacy protection and information security related news or policies updates.
- Regular phishing simulation exercises and security awareness training are conducted to strengthen employees’ ability to identify and respond to social engineering attacks.

Application Security

- HTC adopts a structured Secure Development Lifecycle (SDL) that spans planning, design, development, testing, release, and maintenance phases, with security checkpoints and approvals assigned at each stage for auditability and accountability.
- HTC conducts privacy and information security design reviews during the product design phase to identify potential risks and ensure that products and services meet relevant security and privacy requirements. Before product release, all software must also pass a final security and privacy review, including vulnerability patch verification and security testing, to ensure compliance with regulations and HTC’s internal control requirements.

Data Protection

- All personal and confidential data is protected using strong encryption methods during storage and transmission to prevent unauthorized access or data leakage.
- HTC implements data backup, disaster recovery plans and exercises to ensure business continuity.
- Establish defense mechanisms to prevent the leakage of personal information.
- Keep system logs and perform reviews to ensure abnormal events can be handled appropriately.

Data Retention

HTC has established data retention guidelines that define appropriate retention periods for different types of data based on legal, regulatory, and business requirements. Products and services are required to be securely deleted after reaching End of Life (EOL), in accordance with HTC's data retention guidelines, and considering the nature of the product or service as well as applicable statutory obligations. To minimize risks associated with data over-retention, any data that is no longer necessary is either securely disposed of or properly anonymized.

Vendor Management

To ensure data security, third-party service providers involved in HTC collaborations undergo thorough information security and privacy-related due diligence assessments and reviews. This process includes evaluating their compliance with HTC's security policies and standards, along with ongoing monitoring to mitigate potential risks throughout the partnership.

Infrastructure Availability

The VIVERSE related and other major service's infrastructures are hosted in the trusted cloud environment, which is monitored to detect downtime.

Security Testing

Performing security scans is a mandatory requirement. Depending on the attributes of products and services, HTC has corresponding different security scan type requirements.

- Static Code Analysis
- Host Vulnerability Scan
- Web Application Vulnerability Scan
- Various Device Security Scans
- Container Scan

Risk Assessment

Using a systematic approach to quantitatively assess the potential risks to information assets, including the level of vulnerabilities present in the assets, the types of threats faced, and the severity of potential impacts. Based on the assessed risk levels, further determine whether risk mitigation or risk transfer measures are necessary, In addition to conducting regular information security risk assessments and treatments, risk assessments are also performed if there is a new business or significant change.

Change Management

All system changes must undergo information security risk assessment, and comprehensive change logging and tracking mechanisms enforced.

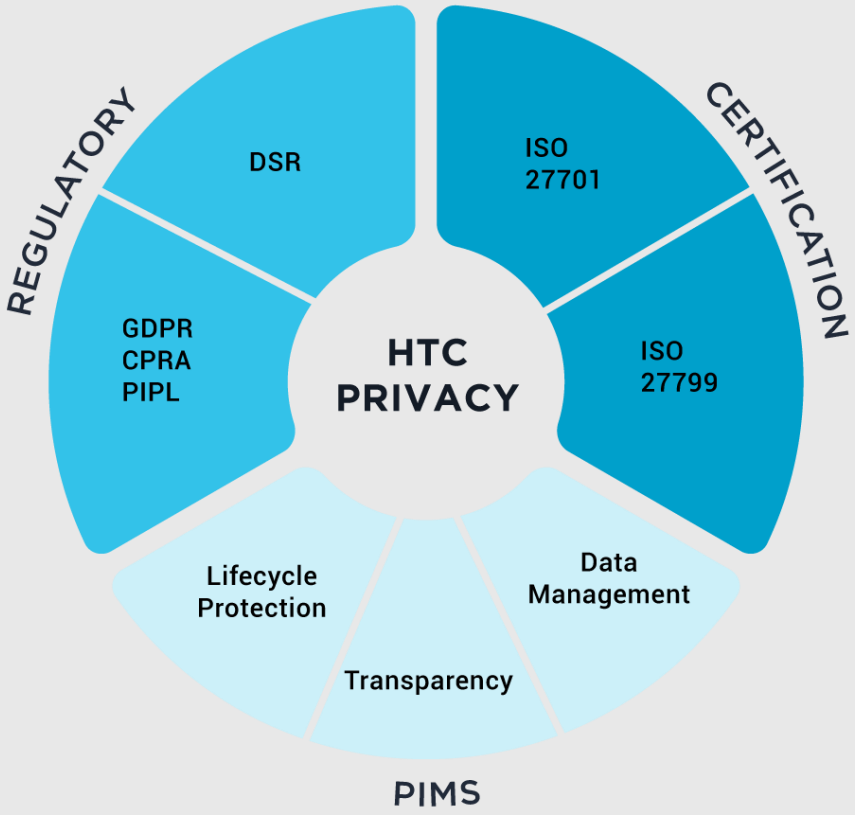
Information Security Incident Management

HTC has established comprehensive incident response policies and procedures designed to address service availability, integrity, security, privacy, and confidentiality issues. To ensure transparency and responsiveness, we provide a public channel, security@htc.com, for promptly reporting security events or incidents handled by our dedicated security team.

Our incident response mechanism is built for rapid and effective action, enabling immediate identification and mitigation of potential threats through continuous monitoring and evaluation. Each incident is thoroughly documented and analyzed, driving ongoing improvements in our security policies and technologies to deliver more secure products and services.

From Design to Delivery — Privacy-First in HTC

At HTC, we believe that technology should serve humanity, not the other way around. Our approach to privacy stems from this belief that people should feel empowered, not compromised, by innovation. In an era where data is abundant and overexposed, HTC is committed to respecting boundaries, safeguarding identity, and enabling imagination through privacy-first design.



HTC is committed to privacy first from design to delivery. It means that every product we develop, every service we offer, and every ecosystem we build is grounded in a proactive commitment to protecting users' data at every stage. Privacy isn't retrofitted, it's engineered into the core of our experiences, ensuring users can trust in their interactions from the moment they pick up a VIVE Intelligent Device, immerse themselves in VIVERSE, or experience the concerts in VIVE Originals.

Our Privacy Information Management System (PIMS) aligns with global privacy regulations and internationally recognized certifications such as ISO 27701 and ISO 27799, reflects our enduring commitment to this privacy-first commitment. PIMS prioritizes transparency, data minimization, and user control, ensuring that privacy is not just a compliance requirement but a key enabler of trust in HTC privacy-first commitment. By embedding privacy-by-design principles into our technology, we create an environment where security is seamless, transparency is standard, and individuals remain in control of their information.

A privacy-first approach is at the core of HTC's responsible innovation principles. These principles are designed to protect user privacy while empowering organizations to explore, connect, and engage with confidence. In our privacy-first approach, we adopt "less is more" to data protection, aligning with the data minimization principle so that we minimize the data processed by our systems to enhance both security and privacy. By handling only the essential data needed for product functionality, we reduce the need for user intervention and provide a seamless experience. This ensures that users can focus on enjoying our products without concerns about complex privacy settings or data vulnerabilities. Effective data protection arises not from adding layers of control but from reducing the overall amount of data handled, allowing for a streamlined, secure system that fuels creativity and innovation.

Privacy Regulations: Building a Global Framework for Trust

HTC's Commitment to Regulatory Compliance

HTC collects, processes, and uses personal data only when there is a lawful basis, adhering to applicable privacy laws, policies, and other legal requirements. We apply the principle of data minimization, ensuring that only necessary data is collected, processed, and used. By limiting data collection to what is essential, we reduce potential privacy risks while enhancing user trust. HTC follows global privacy regulations such as the General Data Protection Regulation (GDPR), which upholds transparency, consent, and data subject rights, the California Consumer Privacy Act (CCPA), which provides users with control over their personal data, and local and regional regulations that protect user rights in various jurisdictions.

Safeguarding Users' Data Subject Rights

Users can request rectification, a copy, or erasure of their personal data through HTC's global email channel, global_privacy@htc.com. HTC commits to responding to these requests within specified legal timeframes. Each request is taken seriously and manually reviewed by HTC's dedicated privacy department team to ensure an accurate and fair response. Unlike many organizations that automate data subject rights (DSR) processes, HTC does not automate its responses, reinforcing our commitment to personalized and thorough data protection. HTC deletes personal data when its collection purpose has been achieved, except when retention is required by law. HTC does not arbitrarily sell users' personal data.

What are ISO/IEC 27701 and ISO 27799

ISO/IEC 27701 is an extension of ISO/IEC 27001, designed to establish a structured framework for managing personal data. It provides a standardized approach to ensuring compliance with global privacy regulations. ISO 27799 complements ISO/IEC 27701 by providing guidelines specifically for health informatics and protecting personal health information within information security management systems.

HTC's Implementation of ISO/IEC 27701 and ISO 27799

HTC has obtained ISO/IEC 27701 certification across various services to enhance its privacy management. This includes conducting privacy risk assessments and implementing controls, clearly defining roles and responsibilities in data protection, and aligning with applicable privacy regulatory frameworks. By undergoing independent assessments and meeting the standard's stringent requirements, HTC demonstrates its commitment to providing greater assurance and credibility.

Additionally, the principles of ISO 27799 are reflected in HTC's approach to safeguarding sensitive data, particularly in contexts involving health and biometric information.

Certification and Continuous Improvement

HTC ensures continuous monitoring and improvement of privacy practices. ISO certification reinforces HTC's commitment to data protection, and we conduct regular internal and external privacy audits and assessments to help maintain compliance and trust.

Privacy Information Management System (PIMS): A Holistic Approach

HTC's PIMS integrates privacy regulations and ISO certification to build a comprehensive system that embeds privacy by design and default into all products and services. It ensures accountability and governance over personal data management and implements secure data lifecycle management. Core aspect of PIMS is **privacy by design**, ensuring privacy is integral to HTC's priority in designing services and products. By reducing the data footprint, we enhance security, simplify compliance, and foster a privacy-centric digital ecosystem that encourages creative exploration without compromising user trust.

Privacy-by-Design from Design to Delivery

HTC's PIMS is embedded at every stage of the product lifecycle, from initial concept and design through development, deployment, and ongoing maintenance, ensuring continuous privacy and security oversight. During the design phase, privacy requirements and risk assessments are integrated into product specifications. In development, privacy controls are implemented alongside functional features, with data flows mapped and tested. Prior to deployment, PIMS governs rigorous validation through privacy impact assessments to certify that privacy safeguards are effective. Once in operation, PIMS provides structured change management, periodic audits, and continuous improvement processes so that updates, patches, and new functionalities maintain compliance with our strict privacy policies and regulatory standards. By applying PIMS end-to-end, HTC guarantees that privacy-first principles are active from design to delivery.

Data Minimization

HTC fully adopts the data minimization principle in privacy by design, ensuring that the collection and processing of personal information are limited strictly to what is necessary for delivering product functionality and user experience. Under this approach:

- HTC processes personal data that is strictly necessary for the intended service or product functionality and avoids collecting or storing unnecessary data.
- Where personal data is not essential for service provision, HTC obtains informed user consent and ensures transparency regarding the purpose and nature of the data collected.
- Sensitive data such as location information is only collected when explicitly enabled by the user, and users are clearly informed about how this data will be used.
- Services are designed to function with anonymous or pseudonymous data wherever feasible, reducing risks associated with identifiable information.

- By minimizing unnecessary data collection, HTC reduces the need for excessive privacy controls and opt-out mechanisms, streamlining user experience while strengthening data protection.

HTC embeds Privacy by Design from the earliest stages of product development by proactively identifying privacy risks, configuring privacy-friendly default settings, applying strong end-to-end security, and ensuring that privacy and functionality are delivered in parallel.

Retention Period

HTC enforces a strict retention policy to support privacy and compliance with global data protection standards.

- Personal data is retained only for as long as necessary to fulfill the specific purpose for which it was collected, based on operational, legal, or regulatory requirements.
- Once the data is no longer needed or upon expiry of the defined retention period, it is securely deleted or irreversibly anonymized in accordance with internal policies.
- All data disposal practices are reviewed regularly and logged to maintain transparency, ensure accountability, and mitigate privacy risks in line with PIMS.

Third-Party Services and Business Partners

For the protection of privacy and information security, HTC sets out strict guidelines in accordance with PIMS for its third-party services and business partners. These third-party services and business partners must fully understand and comply with PIMS requirements. HTC conducts periodic privacy and security assessments with its third-party services and business partners to ensure their continued compliance with PIMS, safeguarding HTC's privacy and information security standards.

User Data Collection and Transparency

HTC is committed to full transparency in its data practices. We publish clear and concise privacy notices that explain what data is collected, how it's used, and who has access. Users and enterprise partners can access intuitive dashboards to view, export, and manage their own data. In addition, HTC issues regular transparency reports detailing government requests, third-party disclosures, and compliance actions. Through these tools and publications, we provide complete visibility into our data handling, reinforcing trust and accountability. Some of the many data collection and transparency designs HTC has in place include:

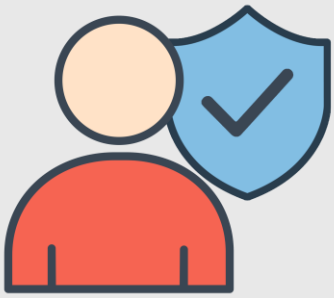
- HTC does not send users' personal whereabouts and location back to HTC without explicit consent. If a fault report is sent with consent, location data is encrypted.
- HTC products and technologies do not process sensitive biometric data such as iris or retina scans without user consent and only for the intended purpose of facial expression tracking.
- HTC does not use user-uploaded photos for biometric identification beyond user's choice of AI services and avatar creation in the VIVERSE ecosystem.
- HTC requires VIVEPORT game developers to provide a privacy policy to ensure transparency when collecting user data.

Secure Software Development in HTC

In the digital age, information security and privacy protection are not just corporate responsibilities but also critical indicators of a company's core values. At HTC, we deeply understand the importance of software product security. Through industry-leading security measures and rigorous development processes, we are dedicated to delivering trustworthy products, safeguarding consumer and enterprise data, and enhancing user experiences.

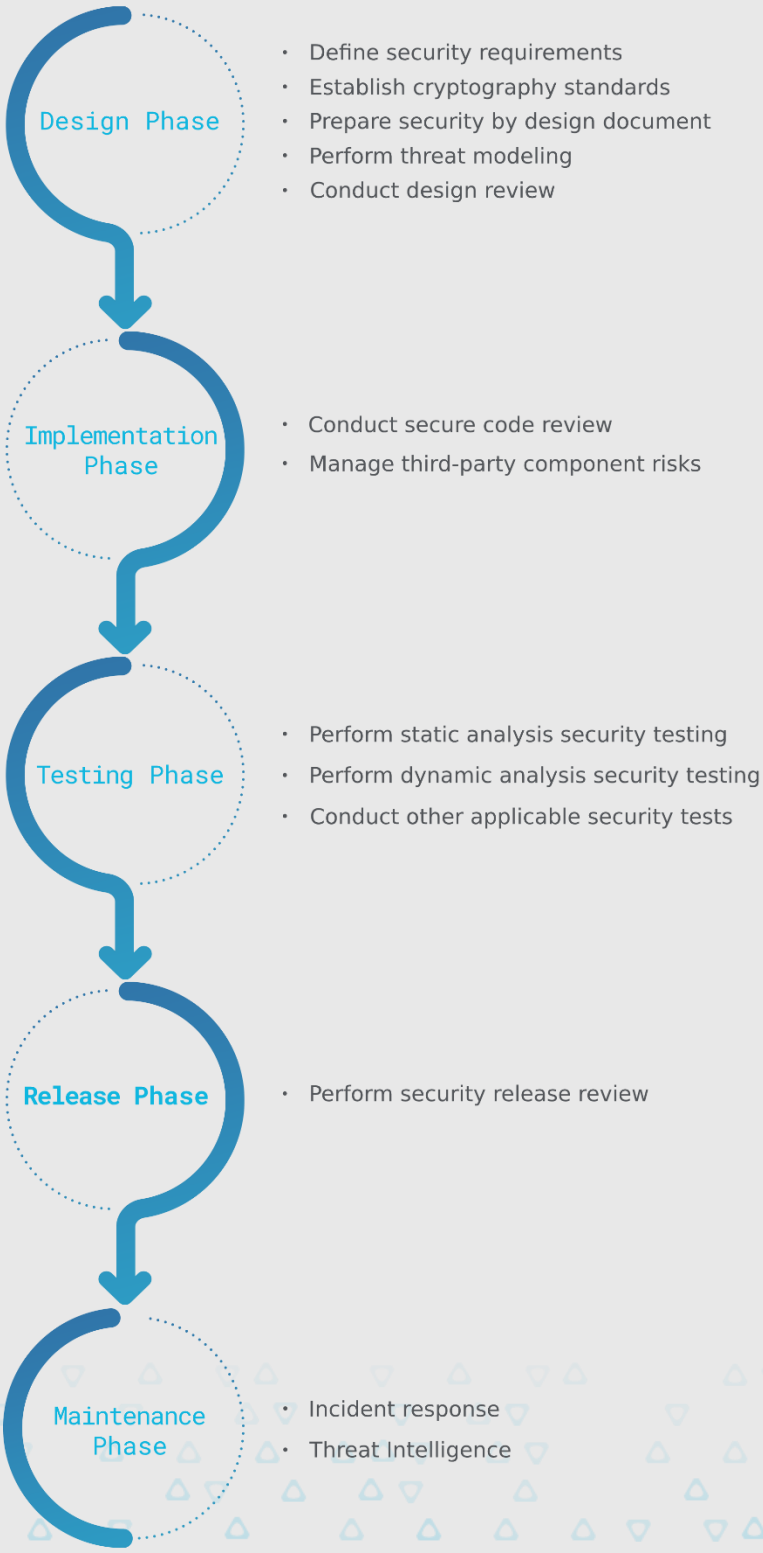
Expert Team Dedicated to Security

Understanding that expertise is fundamental to security quality, we continuously invest in diverse and comprehensive security training resources, providing tailored educational materials for different programming languages and team roles. We regularly review and update training content, conduct periodic training sessions, and continuously assess training effectiveness to enhance our team's security awareness and capabilities.



Our Approach to Secure Software Development

We believe outstanding product security starts with attention to detail in every development phase. Our comprehensive security strategy integrates secure design, secure coding, security testing, and secure release phases, as well as other security controls adopted by the internationally recognized building security in maturity model (BSIMM) framework. To ensure thorough scrutiny at every step, we provide customers with unparalleled product quality and trust.



Advantages of the BSIMM Framework

Utilizing the BSIMM framework, we gain significant strategic advantages:

- **Globally Proven Security Model**: BSIMM's effectiveness is validated by hundreds of global leading enterprises, significantly reducing security risks.
- **Continuous Security Improvement**: BSIMM's systematic assessment allows for continuous evaluation and enhancement of our security maturity, ensuring our products remain at the forefront of security standards.

End-to-End Security Assurance Process

Our robust and transparent security management system adopts BSIMM methodologies throughout all stages of product development:

Secure Design

Proactively identify and mitigate risks early through rigorous data classification and threat modeling

Secure Coding

Adhere strictly to the latest security coding standards to eliminate potential vulnerabilities and threats.

Security Testing

Perform thorough security tests using multiple trusted, industry-recognized scanning tools. This includes open-source software vulnerability scanning to detect known issues. We also integrate AI-driven solutions to assist in vulnerability triage and provide actionable remediation guidance. Our security testing process is routinely executed, especially when new open-source components are introduced or updated, ensuring timely detection and resolution of risks.

Secure Release Review

Execute stringent and comprehensive assessments to confirm compliance with international security standards and ensure the elimination of critical security risks prior to product launch.

Industry Leading Security Practices

We proactively adopt top tier security strategies using advanced technology and international standards to safeguard your information comprehensively:

Comprehensive Sensitive Data Protection

Employing advanced encryption technologies to prevent unauthorized access and personal and business-sensitive data leaks.

Rigorous Open-Source Software Management

Implementing strict management of open-source software to prevent threats from known vulnerabilities effectively.

Advanced Secure Software Lifecycle Management

Implement a structured and comprehensive secure software lifecycle management process, featuring continuous security monitoring, proactive risk management, and adherence to standardized security guidelines. This approach significantly reduces risks at every phase from initial design to post-release maintenance, providing our customers with secure and reliable software products.

Future Vision for Security

We steadfastly uphold our commitment to security excellence and aim to be your most trusted digital partner. Whether you are an individual consumer or an enterprise client, your data security is our highest priority.

HTC Account

The HTC Account system has been meticulously crafted to prioritize user privacy and data protection, ensuring a secure and user-friendly experience across its global data centers. Let's delve into the core aspects of this system, exploring how it handles user information from collection to deletion.

Security and Privacy Measures in HTC Account

Strengthening Data Security

The HTC Account system is built with a robust, multi-layered security framework designed to ensure that user data remains protected at all times. Data transmitted over public networks is secured through HTTPS with advanced encryption protocols, safeguarding confidentiality and integrity during transfer. User data stored within the system is protected using industry-recognized encryption standards, with encryption keys securely managed to prevent unauthorized access. These practices align with international security standards and best practices, reflecting HTC's commitment to safeguarding user privacy and data security.

Strict access control policies are enforced, ensuring that only authorized personnel can access sensitive data. To maintain operational resilience and business continuity, HTC regularly performs disaster recovery and data restoration drills, ensuring rapid recovery and minimal disruption in the event of an incident.

User Control and Data Lifecycle

HTC empowers users with full control over their personal data. Through the HTC Account interface, users can easily view, manage, or request deletion of their information at any time. For additional assistance, users may contact HTC's customer support team, and all deletion requests will be processed in accordance with strict privacy regulations.

Once deletion is finalized, the user's data is permanently removed from active systems, ensuring full compliance with applicable data protection laws and reinforcing HTC's commitment to safeguarding user privacy.

Identity Verification and Protection

The HTC Account system integrates advanced and trusted identity verification mechanisms to ensure account security. OAuth 2.0 is implemented to securely authorize third-party applications without exposing user credentials, maintaining confidentiality and integrity throughout the authorization process.

To further enhance protection, Multi-Factor Authentication (MFA) is enforced using two-factor authentication (2FA) methods. The system architecture is designed with extensibility in mind, allowing seamless integration of additional authentication methods to meet evolving enterprise security requirements.

Access permissions are regularly reviewed to reduce the risks associated with over-privileged accounts, ensuring all access rights adhere to the principle of least privilege and enhancing overall security governance.

Proactive Security Measures

The HTC Account system adopts a comprehensive and proactive approach to security, ensuring protection throughout development and operations. Ongoing security assessments include static code analysis and application-level vulnerability scanning to identify and address potential risks at an early stage.

To safeguard against network-based threats, the system incorporates multiple layers of network defense technologies, including firewall protections, DDoS mitigation strategies, and automated threat detection and response mechanisms ensuring real-time visibility and rapid response to potential incidents.

The physical infrastructure is hosted within cloud environments governed by strict Service Level Agreements (SLAs). Host systems undergo regular vulnerability assessments to maintain system integrity and availability, reinforcing operational resilience and cybersecurity posture.

HTC Account User Data

HTC only collects and uses the personal data in HTC Account for the following purposes:

- To provide and improve HTC products and services.
- For billing purposes.
- To promote safety, integrity, and security.
- To comply with legal obligations.
- Personalized experiences authorized by the users.

Note: User personal data will not be used for personalization of consumer products, advertising, or any purposes beyond those outlined above.

When using VIVE Intelligent Device, data collected for the HTC Account is strictly limited to essential functions:

- Streaming content from VIVE Intelligent Devices to a PC.
- Browsing and purchasing content via the VIVEPORT Store.
- Managing device settings and software updates.

The HTC Account system is not linked to or shared with third-party applications or services, and user data remains confidential. Outside of interactions within the VIVERSE ecosystem, user data is not shared with other users, ensuring that privacy remains a core principle of all VIVE operations.

Compliance and Data Governance

HTC upholds a comprehensive data governance framework founded on accountability, transparency, and user control. Through clearly defined policies and operational procedures, we ensure that personal data is handled in accordance with applicable laws and ethical standards.

To reinforce ongoing compliance, HTC conducts regular internal audits and independent security assessments. These reviews validate that privacy and data protection measures are continuously aligned with global regulations and industry best practices reflecting HTC's unwavering commitment to data security and user trust.

Commitment to Security and Privacy

HTC's dedication to privacy, security, and regulatory compliance is woven into every layer of the HTC Account system's design and operations. Through a systematic security framework and robust governance practices, HTC ensures that user data remains secure, private, and fully under the control of the individual.

This commitment goes beyond policy it represents HTC's response to user trust, consistently upholding the highest standards of data protection and privacy management.

VIVERSE

HTC VIVERSE is an open and immersive metaverse ecosystem that seamlessly integrates Virtual Reality (VR), Augmented Reality (AR), and interactive technologies. It empowers users to create and customize personal avatars, and to explore, socialize, learn, entertain, and work within immersive environment across multiple devices including smartphones, tablets, PCs, and VIVE Intelligent Devices — creating a truly personalized virtual, redefining how people engage with digital worlds.

Through HTC's proprietary VIVEPORT content platform, VIVERSE offers access to thousands of VR applications across diverse categories such as gaming, education, art, cinema, and virtual tourism. This rich content library supports a variety of user needs, from entertainment and learning to creative exploration, enhancing the immersive experience.

For enterprises, VIVERSE enables a wide range of professional use cases, including virtual meetings, online exhibitions, product demonstrations, remote training, and collaborative workspaces. These immersive tools help organizations drive digital transformation, enhance communication, and foster productive, interactive environments. VIVERSE also incorporates enterprise-grade security and privacy measures, ensuring data protection, identity security, and compliance with international standards such as ISO/IEC 27001 and GDPR.

To support developers and creators, VIVERSE offers robust SDKs, APIs, and Create tools—unlocking opportunities to build, expand and innovate within the metaverse ecosystem.

VIVERSE Platform

The VIVERSE Platform is HTC's open and immersive virtual ecosystem, seamlessly integrating virtual spaces, digital identities, and digital asset transactions into a unified experience.

The platform currently consists of three core components: **VIVERSE Worlds**, **VIVERSE Avatar** and **VIVERSE Marketplace**. These components work together to deliver a scalable, interactive metaverse environment for both individuals and enterprises across multiple devices.

All services within the VIVERSE Platform are built upon a consistent and robust security framework, ensuring data protection, user privacy and secure transactions across every interaction.

VIVERSE Worlds

VIVERSE Worlds is a virtual space creation and experience platform. It allows individuals and organizations to build interactive 3D environments, accessible across devices. It is suitable for social gatherings, exhibitions, events, education, and brand engagement.

VIVERSE Avatar

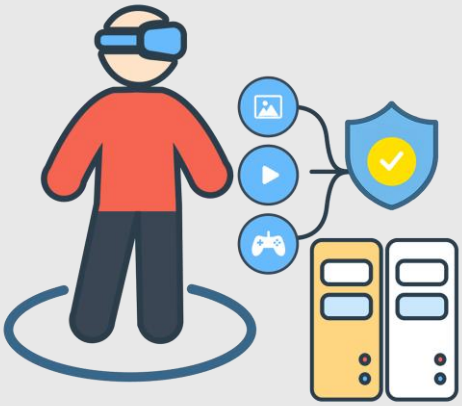
VIVERSE Avatar provides tools for creating personalized 3D digital identities. Users can customize their appearance and expressions, enabling rich interactions across various virtual experiences, including meetings, games, and social activities.

VIVERSE Marketplace

VIVERSE Marketplace is a digital asset trading platform. It allows users to buy and sell virtual items such as avatars, wearables, and environments.

VIVERSE Worlds

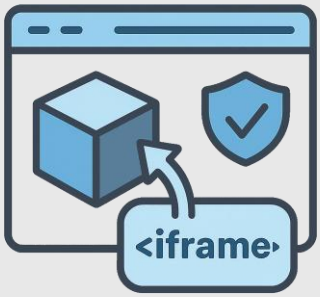
Technology continues to transform how we connect, create, and experience the world around us, and immersive 3D experiences are leading this next wave of digital interaction across industries. VIVERSE Worlds, developed by HTC, is at the forefront of this evolution, offering an advanced open 3D platform that empowers creators, businesses, and users to build, explore, and share digital content seamlessly and securely. Designed for effortless access across smartphones, tablets, PCs, and VIVE Intelligent Devices, the platform eliminates the need for long installations or large data storage, allowing anyone to enter rich virtual environments anytime, anywhere. Whether for gaming, virtual avatars, interactive storytelling, next-generation e-commerce, immersive training, or global virtual events, VIVERSE Worlds provides the foundation for limitless digital engagement. Every interaction is supported by enterprise-grade security and privacy protections, ensuring that digital assets, customer data, and interactive experiences remain consistently safeguarded. From showcasing 3D products to designing immersive landscapes and hosting large-scale audiences, creators and enterprises alike can rely on VIVERSE Worlds to deliver creativity and security in one cohesive experience.



VIVERSE Worlds redefines how digital content comes to life by offering a powerful No-Code Virtual World Builder, VIVERSE Create, that enables creators, innovators, and enterprises to realize their ideas without being hindered by technical barriers, from intuitive template-based world creation for beginners and meetup hosts to advanced integrations with integration and SDKs that enable direct publishing to VIVERSE from different engines. VIVERSE Create offers a comprehensive suite of no-code creator tools that allow creators to build and share interactive multiplayer worlds to any device, anywhere – no code required. Powered by Polygon Streaming technology, the platform delivers stunning visuals and smooth performance even in environments with limited bandwidth. Whether using a high-end workstation or a standard laptop, users enjoy exceptional 3D experiences while knowing their data and creative assets are protected by rigorous encryption and privacy safeguards. Security is embedded into every layer of the platform, ensuring that every interaction remains trusted and protected.

Seamless integration with a wide range of industry-leading 3D development tools and game engines makes VIVERSE Worlds an ideal choice for both individual creators and global enterprises. Supporting VIVERSE Create SDK, PlayCanvas, Wonderland Engine, and Unity for Web, the platform allows projects to be published instantly, eliminating the need for extensive rework. Throughout development and deployment, robust security best practices are enforced, meeting enterprise-grade standards that ensure data integrity and privacy. This approach enables creators and businesses to focus on innovation and storytelling with confidence that their work is safeguarded at every step.

Sharing immersive content through VIVERSE Worlds is designed to be both intuitive and secure. With a single line of iFrame code, creators can seamlessly embed interactive 3D experiences into any website, extending their reach to global audiences without compromising content integrity or confidentiality. Each layer of data transmission and interaction is rigorously protected, ensuring that creators retain full control over their work while delivering reliable, seamless, and engaging digital experiences.



Personal identity within the VIVERSE Worlds ecosystem is equally respected and protected. Users can create and customize avatars to represent their unique selves across virtual spaces, enhancing engagement and interaction. Behind these experiences lies a steadfast commitment to privacy, ensuring that personal data remains secure as users explore and connect in new digital environments.

VIVERSE Worlds represents more than just a platform. It is the future of immersive digital interaction, blending creativity, accessibility, and trust into one cohesive experience. By making 3D content creation and sharing more accessible while embedding enterprise-grade security throughout, VIVERSE Worlds gives businesses, developers, and creators the tools to innovate freely, knowing their work is always protected.

Security and Privacy Measures in VIVERSE Worlds

Authentication & Authorization

- Users authenticate with their HTC account before accessing their personal data.
- Authentication and authorization are securely managed in the backend using industry standard protocols.
- Any request involving user data requires validated access tokens to ensure proper authorization.

Data Protection and Encryption

- User data is securely stored in Amazon Relational Database Service with encryption, regular backups, and built-in AWS security features ensuring protection.
- All data transmissions use secure transport protocols adhering to recognized encryption standards, providing strong protection against unauthorized access.

File Security and Storage

- Files are safely stored in Amazon S3 or Amazon EFS, with strict access controls to prevent unauthorized access.
- Access to file storage is tightly managed to prevent unauthorized usage.

Error Handling and Secure Logging

- Error messages presented to users are carefully designed to prevent the disclosure of sensitive information.
- System logs are securely maintained with controlled access, ensuring operational visibility without compromising security.

Cross-Origin Resource Sharing

CORS policies are configured to allow resource access only from trusted domains, reducing exposure to unauthorized cross-origin requests.

Third-Party Service Integration

Integrations with third-party service integration uses dedicated access tokens with limited scopes and controlled permissions to ensure secure and isolated interactions.

Secure Coding Practices

- Sensitive data such as passwords, API tokens, and private keys are never committed to source code repositories.
- Development follows secure coding guidelines to minimize risks and maintain system integrity.

No Retention of Communication Data

HTC does not store or transfer to third party any user's communication data such as text messages and voice communication. Users can freely express and communicate in VIVERSE Worlds without worrying about their communication data being processed for any other purposes.

Privacy Controls of the User's Content

Users can choose to set their content to private, unlisted, or public. In Private setting content can only be accessed by the owner. In unlisted settings, content can be accessed by the owner and visited by others via a sharable link. In Public setting, content is available to everyone, which means visitors will be able to like and see the user's content.

VIVERSE Avatar

VIVERSE Avatar is a powerful creation tool designed to help you authentically express your individuality in the virtual world. Whether you're exploring the VIVERSE ecosystem or engaging in virtual experiences, your avatar becomes a reflection of your unique style and personality. Choose from a wide range of built-in characters or upload your own custom 3D digital persona using the VRM standard, ensuring your identity stays consistent across different platforms and services.

The platform offers flexible tools for crafting dynamic avatars that match your personal style. With diverse styling options, you can select from refined VIVERSE-styled avatars, playful cartoon-like designs, or hyper-realistic representations to fit any virtual environment or interaction. VIVERSE Avatar also supports the open VRM format, allowing seamless integration of avatars from other platforms so you can maintain your digital identity wherever you go.

Beyond customization, VIVERSE Avatar connects to the broader VIVERSE Marketplace, where you can trade and exchange avatar-related digital assets using VIVERSE points. This makes it easy to expand your virtual wardrobe and enhance your digital presence, offering a flexible and connected avatar experience within the metaverse.

Security and Privacy Measures in VIVERSE Avatar

Data Storage Encryption

- **Data at Rest**: All user data stored within the platform is encrypted at rest using cloud-native encryption services, with encryption keys managed securely through industry-standard key management systems. This ensures that data remains protected against unauthorized access at the storage layer.
- **Data in Transit**: Data transmitted between services and users is secured through robust encryption protocols, ensuring confidentiality and integrity across the network. These protocols follow recognized security best practices and employ modern cryptographic algorithms.

Data Backup and Disaster Recovery

- Automated daily backups are performed and retained for a defined period to ensure data availability.
- A comprehensive disaster recovery plan is in place, designed according to HTC and industry standards for high availability and data integrity. Regular drills and testing are conducted to verify that services can be rapidly restored in case of unexpected events.

Network Security

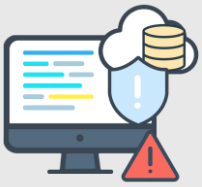
- **Web Application Firewall (WAF)**: The platform employs a WAF to enhance security at the application layer, protecting against common web threats and attacks.
- **Secure Communication**: All communications between clients, services, and servers are protected using industry-standard encryption protocols that ensure data confidentiality and integrity.

Vulnerability Management

Regular vulnerability scanning is performed across code, host environments, and application layers. This includes monthly code scans, periodic host vulnerability assessments, and black box testing to identify and remediate potential risks.

Cloud Infrastructure Security

- **Access Control**: Employs Amazon IAM services for access rights management to ensure secure authorization and authentication.
- **Monitoring and Log Management**: Uses Amazon CloudWatch infrastructure is continuously monitored, and security scans are regularly performed on container images to maintain a secure environment.



Log Management and Monitoring

- **Log Scope**: Comprehensive logging covers application, system, and network activities, including HTTP access logs, application logs, database logs, and security events.
- **Event Logging**: Key actions such as user login, data access, and error events are logged for traceability.
- **Retention and Monitoring**: Logs are securely stored for a defined retention period and regularly reviewed to detect abnormal activities and potential risks.
- **Centralized Analysis**: Logs are centrally managed and analyzed through advanced monitoring tools, with secure access controls and encryption applied to log data. Alert mechanisms are in place to promptly respond to critical events such as system errors or suspicious behavior.

User Photo and Realistic Avatar

VIVERSE Avatar offers users the option to create personalized and realistic avatars by uploading a photo of themselves. This feature allows for a more immersive and engaging experience across the VIVERSE platform, reflecting the user's likeness in virtual environments.

HTC is committed to ensuring that this personalization capability does not come at the expense of user privacy. When a user uploads a photo to generate their avatar, the image is processed solely for the purpose of creating the avatar. Once the processing is complete, the photo is automatically deleted and is not stored by HTC.

This privacy-focused design ensures that no biometric or image data is retained beyond its immediate use. HTC does not use these photos for identification, profiling, or any secondary purposes. By adopting a strict data minimization approach, HTC reinforces user trust while delivering advanced personalization features.

Through these comprehensive security measures, VIVERSE Avatar ensures robust protection across data security, network security, application security, and infrastructure security. This framework safeguards users' digital personas, preserves personal privacy, and protects valuable data assets, providing a secure and reliable foundation for virtual interactions.

Whether for engaging with friends in immersive digital spaces, exploring endless virtual possibilities, or creating branded virtual identities, VIVERSE Avatar offers a trusted and flexible gateway into the metaverse.

VIVERSE Marketplace

VIVERSE Marketplace is an integrated digital assets trading platform within the VIVERSE metaverse ecosystem, designed to provide users with a secure and seamless environment to buy, sell, and showcase digital collectibles. It enables users to complete purchases conveniently with standard payment methods, including credit cards, while ensuring secure management of their digital assets.

Within VIVERSE Marketplace, users can explore a diverse range of digital assets, including artwork, music, virtual fashion items, and more, all designed to enhance experiences within the VIVERSE virtual world.

The launch of VIVERSE Marketplace represents HTC's strategic expansion into the metaverse economy, fostering an open, accessible, and diverse virtual ecosystem. By enabling users to create, trade, and showcase digital content, the platform bridges the gap between virtual interactions and real-world ownership, promoting a vibrant community of creators and collectors.

Key features

- **Digital Asset Trading**: Users can purchase and trade digital artworks, virtual fashion items, and other virtual goods from VIVERSE ecosystem partners and utilize these assets within the VIVERSE virtual world.
- **Secure Asset Management**: VIVERSE Marketplace ensures secure storage, management, and transfer of virtual assets, providing users with a reliable and flexible ownership experience.
- **Convenient Payment Options**: Transactions can be completed using standard payment methods such as credit cards, offering a convenient purchasing experience for users across different markets.

Security and Privacy Measures in VIVERSE Marketplace

Encryption Strategy

Data stored within the VIVERSE Marketplace platform in Amazon RDS is encrypted by default using industry-standard encryption services. Encryption keys are securely managed through Amazon Key Management Service (KMS), providing strong protection for data at rest and in transit. These practices align with global security standards and best practices.

Data Backup and Restoration

Automated daily backups are maintained and retained in accordance with HTC's internal policies and data governance standards. A comprehensive disaster recovery framework is established, including regular drills and recovery validation tests to ensure service continuity during unexpected incidents. The system is designed to meet high availability and data integrity requirements in line with HTC and the industry's best practices.

Network Boundary Protection

Multiple layers of network defense are implemented, including firewall configurations and intrusion detection/prevention systems. Web application protection mechanisms are also in place to detect and block common attack vectors at the application layer. All configurations are periodically reviewed to maintain effectiveness against evolving threats.

Secure Communication Protocols

Communications across the platform are protected using advanced encryption protocols supporting multiple modern cryptographic algorithms. These protocols provide confidentiality, integrity, and authentication across all data transmissions and are regularly reviewed to remain compliant with evolving security standards.

Vulnerability Management

Regular source code scans, host vulnerability scans, and black-box testing ensure a comprehensive security assessment and proactive threat mitigation.

Cloud Infrastructure Security

The platform enforces strict identity and access management policies and employs continuous monitoring to ensure infrastructure health and threat detection. Alerts and automated safeguards are in place to maintain system resilience and operational reliability.

Container Security

Containerized components undergo regular image scanning and are governed by granular access control policies. These measures ensure secure deployment and runtime isolation within the virtualized environment.

Log Management and Monitoring

Logging is implemented across the application, system, and network layers to capture critical events such as authentication attempts, data access, and system errors. Logs are securely synchronized and retained in accordance with defined policies, with regular anomaly detection reviews conducted to identify potential security threats.

Centralized Logging and Alerting

A centralized logging system is deployed to enable real-time monitoring and forensic analysis. Log data is encrypted in transit and at rest, with access strictly restricted based on roles. Automated alert mechanisms are configured to flag unusual activities, such as privilege escalations or unauthorized access attempts.

VIVERSE Marketplace is built with a strong emphasis on security and privacy. All transactions are protected using secure encryption protocols, and wallet integrations adhere to industry best practices for safeguarding digital assets. User privacy is prioritized throughout the platform's design, and personal and transactional data are handled in compliance with applicable privacy regulations, ensuring a safe and trusted environment for digital commerce within the VIVERSE ecosystem.

VIVERSE for Business

VIVERSE for Business is an enterprise-focused metaverse platform. It enables businesses to engage in immersive virtual spaces to conduct a variety of business activities, such as virtual meetings, training, product showcases, and collaborative workspaces. The platform enhances engagement, collaboration, and productivity for both in-person and remote work scenarios, while maintaining enterprise-grade security and privacy protections to safeguard business data and communications.

VIVERSE for Business offers an enterprise-ready solution for organizations to create immersive virtual spaces for businesses' employees, customers, and business partners. The platform provides tools for building customized 3D environments with branded visuals using a modular system. Users can access VIVERSE for Business through VIVE Intelligent Devices, computers, and mobile devices, with security embedded across all access points and interactions.

Key Features

- **Customizable Virtual Environments**
  Businesses can design tailored 3D spaces to align with their branding and operational needs, such as virtual offices, training rooms, or showrooms.

- **High-Fidelity 3D Models**
  With advanced Polygon Streaming technology, users can interact with detailed 3D models and visuals seamlessly across devices, ensuring smooth and reliable performance.

- **Cross-Platform Accessibility**
  The platform supports VIVE Intelligent Devices, computers, and mobile devices, providing consistent access regardless of location or device type.

- **Immersive and Interactive Features**
  Tools for real-time interaction, avatar customization, and engaging virtual experiences foster deeper connections between employees, partners, and clients.

- **Virtual Collaboration**
  Teams can connect within immersive virtual environments to collaborate on projects or hold productive meetings, bridging geographical distances.

- **Training and Education**

  Interactive VR training sessions support onboarding, skill development, and product education, offering scalable solutions beyond physical spaces.

- **Product Demos and Showcases**

  Present and interact with 3D product models, delivering engaging demonstrations to clients or partners.

- **Hybrid Workspaces**

  Enable seamless collaboration between remote and in-office employees, enhancing productivity with immersive tools.

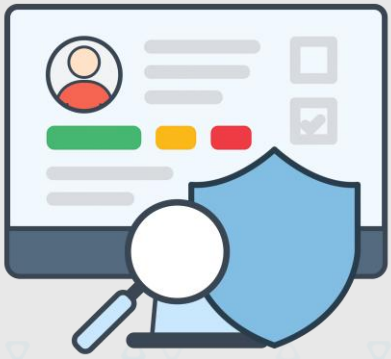
- **Enterprise-Grade Security and Privacy**

  All data, assets, and communications within VIVERSE for Business are protected by robust security frameworks, including encryption, secure authentication, and privacy controls that align with global standards, ensuring safe and trusted virtual interactions.

Security and Privacy Measures in VIVERSE for Business

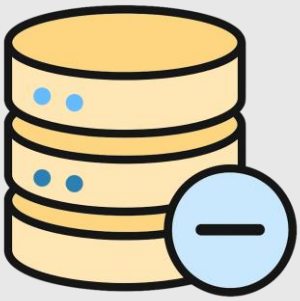
Security is a priority for VIVERSE for Business, with robust measures in place to protect data at every level. VIVERSE for Business applies advanced encryption techniques to safeguard data at rest and data in transit, ensuring that all information remains secure and confidential throughout its lifecycle. These protections follow recognized industry standards and are continuously evaluated to align with evolving security best practices. Access to data is strictly controlled using Role-Based Access Control (RBAC). Each business tenant's data is securely isolated to prevent unauthorized access. The platform also supports Single Sign-On (SSO) integration with enterprise identity providers like Azure AD for secure authentication. VIVERSE for Business enforces Multi-Factor Authentication (MFA) with 2FA via SMS and/or Email for an additional layer of security. Administrators can also define and manage permissions at the user and group levels.

VIVERSE for Business infrastructure is hosted on the secure and compliant Amazon Web Services. Regular security vulnerability assessments and security testing are conducted to identify and mitigate risks. The platform employs network security measures, including multiple layers of network security controls to monitor, detect, and prevent unauthorized activities. VIVERSE for Business adheres to international standards for information security management with ISO/IEC 27001 and ISO/IEC 27701 certifications verified by independent auditors.



VIVERSE for Business uses a secure, enterprise-level, web-based Management Console that allows authorized members with authorized administrators with defined roles and permissions to manage their virtual environment and member permissions. Advanced monitoring tools are used to detect and respond to security threats in real-time. A well-documented incident response plan is in place to promptly address and mitigate security incidents. Comprehensive audit logs are maintained for system activity to enable traceability and forensics.

VIVERSE for Business is regularly updated and patched to ensure security against known vulnerabilities. Automated backups of critical data with secure storage solutions and a comprehensive disaster recovery plan are in place.



HTC has implemented a strict data non-retention policy for VIVERSE for Business. VIVERSE for Business does not store or retain users' real-time streaming content, audio or video communications, or meeting interaction data. This means that any communication or content shared during VIVERSE for Business meetings is ephemerality exists only during the live session and is not recorded, saved, or processed for secondary purposes.

By not retaining communication data, HTC significantly reduces privacy risks and enables organizations to operate in a secure digital environment. This approach aligns with HTC's data minimization principle and ensures that sensitive business information, internal discussions, or personal interactions are not subject to unnecessary storage or processing

VIVERSE Polygon Streaming

VIVERSE Polygon Streaming is an advanced 3D rendering technology, designed to elevate the visual quality and performance of virtual worlds and online experiences. By storing high-resolution 3D models in the cloud and intelligently streaming only the necessary portions based on the user's perspective and device capabilities, the technology significantly reduces the processing load on local devices while delivering a low-latency, high-fidelity 3D experience.

Key Features

- **Occlusion Culling**: Only renders objects within the user's current field of view, skipping hidden or irrelevant elements to optimize resource usage and enhance rendering performance.
- **Adaptive Level of Detail (LOD)**: Dynamically adjusts the complexity of 3D models based on the device's hardware capabilities and network conditions, ensuring optimal visual performance across a variety of platforms.

Benefits

- **Cross-Platform Compatibility**: Provide consistent, high-quality 3D visuals across a wide range of devices, including high-performance PCs, tablets, smartphones, and VIVE Intelligent Devices, minimizing the need for high-end hardware investments.
- **Improved Loading Efficiency**: Reduces loading times by up to 8 times, boosts average frames per second (FPS) by up to 2 times, and decreases project file sizes by up to 81%, resulting in a significantly improved user experience with faster access and smoother interactions.

Security and Privacy Measures in Polygon Streaming

Encryption Strategy

Data stored within the platform in Amazon RDS is encrypted by default, with encryption keys securely managed using industry-standard Amazon Key Management Service (KMS). Encryption is enforced both at rest and in transit to ensure the confidentiality and integrity of sensitive information.

Data Backup and Restoration

- Automatic daily backups are maintained and retained in accordance with best practice retention policies to ensure data availability and resilience.
- A comprehensive disaster recovery framework is established, with regular drills and testing conducted to validate recovery procedures. The entire system is designed to meet HTC's internal standards and align with industry best practices for high availability and data integrity.

Network Boundary Protection

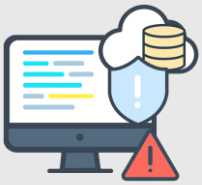
- Robust firewall configurations and intrusion detection/prevention systems (IDS/IPS) are deployed to secure network perimeters, with regular reviews to maintain their effectiveness. AWS Security Groups serve as the primary boundary protection mechanism, and their configurations are periodically reviewed to ensure continued security.
- Web application protection services are actively utilized to defend against web-based threats, with the AKAMAI WAF service specifically deployed for comprehensive web application security.

Secure Communication Protocols

- Communications across the platform utilize secure, standards-based encryption protocols, ensuring that data in transit remains protected against unauthorized access.
- These protocols are continuously reviewed and updated to meet evolving security requirements and emerging threats landscapes.

Vulnerability Management

Regular source code scans, host vulnerability scans, and black-box
testing ensure a comprehensive security assessment and proactive threat mitigation.



Cloud Provider Security Measures

Identity and access management are enforced using Amazon IAM, providing robust control over user permissions and access. Continuous monitoring is achieved through Amazon CloudWatch, ensuring service reliability and enabling early detection of anomalies within the cloud infrastructure.

Virtualization and Container Security

Container security is maintained through regular scans of container images and strict access control policies, safeguarding the platform's virtualized environments.

Log Management and Monitoring

Extensive logging is implemented across application, system, and network layers, capturing key security events such as user authentication activities, data access, and system errors. Logs are securely synchronized and retained in accordance with internal policies, with regular reviews conducted to detect potential anomalies.

Centralized Logging and Threat Monitoring

- Centralized log management and analysis are deployed to enhance visibility and traceability across the environment.
- Secure transmission and storage of logs are enforced with stringent access controls, and alert mechanisms are established to monitor and respond to critical security events, including privilege escalations.

VR Content Stores

VIVEPORT is a leading digital distribution platform and online store for Virtual Reality (VR) content, offering access to a wide range of VR applications, games, videos, and immersive experiences across categories such as entertainment, education, productivity, and more. It supports a diverse array of VR devices, including HTC VIVE systems, Meta Quest (via PCVR link), and other major VR hardware, providing a flexible and accessible ecosystem for VR users.

VIVEPORT empowers developers by providing tools and resources to publish, promote, and monetize their VR applications, contributing to the growth of a vibrant VR content ecosystem. General users can choose from flexible membership options to access a curated library of VR apps and games, including new releases and exclusive titles. The platform is designed to make VR content more accessible, enhancing the reach of high-quality immersive experiences across global audiences.

VIVE Business AppStore serves as a dedicated enterprise marketplace within the HTC VR ecosystem, offering a comprehensive selection of software solutions and tools tailored for businesses and industries. Focused on sectors such as healthcare, education, training, design, simulation, retail, manufacturing, and real estate, the AppStore delivers professionally vetted applications including training simulations, 3D design tools, collaborative VR meeting software, and more. Businesses can leverage flexible, subscription-based licensing models designed to support enterprise-scale deployment and operational needs.

Both VIVEPORT and the VIVE Business AppStore are essential pillars of the VIVERSE ecosystem, ensuring access to high-quality, professionally reviewed applications that drive innovation, productivity, and immersive engagement in both consumer and enterprise markets.

Security and Privacy Measures in VIVEPORT and VIVE Business AppStore

Privacy-First Platform Architecture

The VIVEPORT and VIVE Business AppStore platforms are built with privacy and security at their core, adhering to the highest international standards. Both platforms are designed to give users control over their personal information while maintaining a secure, trusted environment.

Network and Application Security

- The platforms employ a robust multi-tiered defense strategy, including the use of web application firewalls (WAF), distributed denial-of-service (DDoS) protection, and regular security scanning to detect and proactively mitigate vulnerabilities.
- API input validation is enforced to prevent malicious attacks.
- A content delivery network (CDN) integrates WAF protections to guard against SQL injection and other common threats.
- Role-based access controls restrict access sensitive information, minimizing the risk of accidental data exposure.

Data Handling and Protection

- The platforms use secure, tested components in both front-end and back-end systems.
- Redundant systems across the CDN, load balancers, and database infrastructure prevent single points of failure, ensuring service availability even during hardware or software failures.

Data Protection

- Data in Transit: Data transmitted between users and the platform is protected by secure communication protocols utilizing advanced encryption standards, ensuring confidentiality and integrity throughout the transfer process.
- Data at Rest: Data stored within the platforms is safeguarded using cloud-native database encryption mechanisms.
- Key Management: Encryption keys are securely managed through industry-standard key management systems to prevent unauthorized access.
- Compliance: Data protection measures align with recognized international security standards and best practices.

Fail-Secure Mechanisms

- User accounts are automatically locked after a defined number of failed login attempts to mitigate brute-force attacks.
- APIs are configured to automatically block IP addresses exhibiting abnormal error behaviors, further enhancing system resilience.

High Availability and Redundancy

- Redundant systems are deployed across all infrastructure layers, including multiple Akamai CDN edge networks, Amazon load balancers, and Kubernetes clusters, ensuring uninterrupted service delivery even during component failures.
- Databases operate in clustered architectures to provide automatic failovers and maintain data integrity.

Disaster Recovery and Business Continuity

HTC has established a comprehensive disaster recovery plan (DRP) to ensure rapid recovery and minimal disruption in the event of unplanned incidents. Regular disaster recovery drills are conducted for both VIVEPORT and VIVE Business AppStore to validate the effectiveness of recovery procedures and maintain compliance with business continuity standards.

Privacy Enforcement on Third Party Developers

Third-party apps on the VIVEPORT adhere to their own terms and privacy policies. However, HTC enforces the VIVEPORT Platform Terms and Developer Policies, reserving the right to remove non-compliant apps or developers. Sensitive or proprietary information shared with third-party apps is processed solely by the app developer, in accordance with their terms. HTC does not access data processed on the app layer.

At VIVE Business Appstore and VIVEPORT, security and privacy are fundamental to our platform design and operations. Through the implementation of comprehensive privacy and security controls, robust access management, and adherence to international privacy standards, we ensure that user and enterprise data are protected across every stage of interaction. Our commitment to transparency, continuous security enhancements, and proactive risk management enables organizations and users to trust VIVE Business AppStore and VIVEPORT as secure, reliable environments for business and immersive experiences. We remain dedicated to the ongoing evaluation and improvement of our security strategies to uphold the highest standards of data protection practices and platform integrity.

VIVE

HTC VIVE has long been committed to advancing new paradigms of human-technology interaction, and the VIVE Intelligence Devices embody our vision for the next generation of human-machine interfaces. Seamlessly integrating perceptual technologies, spatial computing, and environmental awareness, VIVE Intelligent Devices serve as critical bridges between virtual and physical worlds. Designed for versatility, VIVE Intelligence Devices operate across diverse scenarios such as personal entertainment, remote collaboration, creative development, professional training, and real-time navigation, becoming indispensable intelligent nodes that support both work and daily life. Beyond delivering immersive experiences and real-time interaction, they enable users to access information, connect with resources, and make informed decisions anytime and anywhere, significantly enhancing flexibility and operational efficiency.

HTC remains steadfast in our commitment to a people-centric, experience-first design philosophy across all products. VIVE Intelligence Devices are engineered with security and privacy protections deeply integrated from system architecture to user workflows, ensuring that every interaction remains safe, reliable, and trustworthy. As the world moves toward a future of intelligent connectivity, HTC continues to innovate with purpose, helping individuals and enterprises establish a secure, scalable, and dependable foundation for the intelligent era ahead.

VIVE AI

VIVE AI is an innovative solution that integrates smart glasses, a mobile application, and cloud-based AI technologies. It consists of VIVE Eagle (smart glasses), VIVE Connect (mobile application), and a cloud AI service platform, delivering intelligent assistance, smart photography, real-time translation, and voice interaction. Powered by HTC's proprietary VIVE AI Voice Assistant, users can quickly record to-do lists, locate parked cars, look up destinations, or get restaurant recommendations through simple voice commands. This allows them to stay focused on the moment and makes VIVE AI more than just a voice assistant, serving as a smart note-taking companion for life on the go.

Unlike most smart glasses on the market, VIVE AI integrates an on-device Nudity Detection feature that identifies images potentially containing nudity without disrupting the user experience. All analysis is performed locally on the device, ensuring that no photos or videos are ever transmitted to the cloud.

Privacy and Security by Design with Comprehensive Protection

HTC has consistently upheld the highest standards in protecting user information. From the very beginning, VIVE Eagle was designed with personal privacy as a core priority. All user data is stored exclusively on the device, never used for behavioral tracking, and never utilized for training any AI models. When using our Large Language Model (LLM) services, the system is designed so that they cannot trace any activity back to you personally, ensuring your privacy is fully protected. This means you can enjoy powerful AI assistance and immersive experiences with complete peace of mind, knowing your world stays yours alone.

The product employs AES-256 encryption compliant with U.S. NIST standards, an algorithm approved by the U.S. National Security Agency (NSA) for securing Top Secret–level information. This advanced protection safeguards your data during local storage and greatly reduces the risk of leakage.

The frame features a built-in LED capture indicator that lights up whenever photos are taken or videos are recorded, making every capture transparent. If the glasses are not worn or the indicator light is covered, capturing is simply not allowed. In these situations, recording is strictly prohibited and cannot be bypassed, ensuring that no unintentional shots are taken and that the privacy rights of everyone around you are fully respected at all times.

VIVE AI has achieved ISO/IEC 27001 Information Security Management System and ISO/IEC 27701 Privacy Information Management System certifications, as recommended for issuance by SGS. These certifications demonstrate compliance with globally recognized standards for information security and personal data protection. From the design stage, the product has followed Security by Design principles to ensure an optimal balance between innovative functionality and user privacy.

Security and Privacy Measures in VIVE AI

At VIVE AI, we adopt Security by Design as a core engineering principle, ensuring that security is considered at every stage of the system lifecycle from planning, development, and testing to deployment and operations. This approach aligns with international security standards and ensures that every component, process, and data flow is inherently resilient against threats. By embedding security from the outset rather than adding it later, VIVE AI delivers innovative user experiences while maintaining a high level of protection.

In line with the Security by Design approach, VIVE AI incorporates the following core principles:

Strengthen the Weakest Link

Secure potential entry points through Bluetooth pairing encryption, local data encryption, and signed firmware update verification.

Defense in Depth

Apply layered protections across hardware, application, cloud, and network layers so that the failure of one defense does not compromise the entire system.

Separation of Duties

Clearly separate the roles and privileges of the smart glasses, mobile application, and cloud platform to prevent misuse or unauthorized access.

Least Privilege

Grant only the minimum permissions required for users, system modules, and cloud service accounts to perform their intended functions.

Fail Secure

Automatically block or revert operations to a secure state if validation fails, tokens expire, or anomalous responses occur.

Complete Mediation

Revalidate identity and authorization for every request without relying on prior approvals.

Open Design

Use recognized industry standards such as TLS and AES encryption instead of proprietary or obscured methods.

Secure Defaults

Require authentications for all APIs, enforce encrypted connections, and block unsupported HTTP methods by default.

Leverage Proven Components

Utilize the security capabilities built into the platform and cloud services to minimize the risk of unknown vulnerabilities.

User-Friendly Security

Provide clear recording indicators and perform automated background security checks to reduce user burden.

Security & Privacy Controls

VIVE AI applies multi-layered security controls across the device, application, and cloud platform to ensure protection at every stage of data handling and system operation.

VIVE Eagle

Data Protection

All images and audio are stored in the application sandbox. When temporary storage is required, files are encrypted using AES-GCM and automatically deleted after use.

Secure Communication

BLE connections are protected by encrypted pairing, and Wi-Fi transfers use TLS 1.3 for end-to-end encryption

Firmware Updates

Only officially signed firmware images are accepted. If validation fails, the system reverts to the last stable version.

Recording Transparency by Design

A blinking LED alerts others when the camera is active, while the proximity sensor automatically stops recording if it is covered.

Single-user Model

If another user attempts to pair with your VIVE Eagle, all stored data on VIVE Eagle is automatically erased.

VIVE Connect

Authentication

Uses OAuth 2.0 with Two-Factor Authentication (2FA) and short-lived tokens that are refreshed periodically.

Secure Communication

All cloud connections require HTTPS/TLS, and server certificates are validated to prevent MITM attacks.

Minimal Permission Access

Requests only the essential OS permissions and verifies device integrity before enabling sensitive features.

Privacy Controls

Camera and microphone features are enabled only with explicit user consent.

Nudity Detection

All photos and videos are analyzed locally on the device and are never uploaded to the cloud.

Exclusive Photo Management

Photos are kept in a secure, app-specific gallery, inaccessible to third-party apps unless you choose to share.

Cloud AI Service Platform

Identity and Access Control

All APIs use token-based authentication combined with IP allowlisting to ensure that only authorized clients can connect.

Data Protection & Encryption

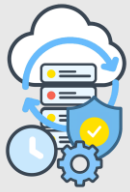
All in-memory data stores and cloud storage services apply transparent encryption at rest and TLS encryption for data in transit, safeguarding information end to end.

Network Defense

Implements strict network controls, including limiting open ports, applying CDN-level rate limiting, filtering unsupported HTTP methods, and deploying both Web Application Firewall (WAF) and DDoS protection.

AI Content Safety

Uses preconfigured prompts to prevent users from injecting additional actions, while leveraging the AI model's built-in safeguards against prompt injection to protect sensitive data.



Disaster Recovery and Business Continuity

Maintains tested plans and mechanisms that ensure rapid recovery and uninterrupted operation during system failures, security incidents, or natural disasters.

Cloud Infrastructure Security

Built on secure, globally recognized cloud infrastructure with compliance to international security and privacy standards.

De-Identification

Ensure de-identification before accessing any third party.

Security Validation and Testing

The security of VIVE AI is maintained through a rigorous and continuous validation process designed to ensure resilience against emerging threats and alignment with international security standards.

Threat Modeling

Performs structured risk assessments before releasing new features, identifying potential vulnerabilities and defining targeted mitigation strategies.

Static Application Security Testing (SAST)

Analyzes application and backend code early in the development cycle to detect and remediate security issues before deployment.

Mobile Application Security Testing

Uses specialized tools to evaluate Android and iOS application packages, reviewing code structure, permission usage, configuration security, and dependencies as part of comprehensive security validation.

Component Scanning

Identifies known vulnerabilities in third-party libraries and container images, ensuring insecure components are updated or replaced promptly.

Container Security

Conduct in-depth assessments of container images and runtime environments to detect misconfigurations, vulnerabilities, and compliance gaps.

VIVE Intelligent Device Series

VIVE is committed to providing a secure, reliable, and privacy-first platform that enables users and enterprises to focus on creativity, innovation, and intelligent operations. By prioritizing data protection and implementing rigorous security measures, VIVE Intelligent Devices empower businesses to confidently harness the potential of VR, AR, and AI technology.

For enterprises, the VIVE Intelligent Device serves as a critical technological foundation for digital transformation and intelligent operations, enabling future-ready workflows such as remote assistance, simulation-based training, and mobile productivity. With its reliable performance, secure architecture, and open platform, this all-in-one XR lineup is more than just hardware. It is a strategic gateway for businesses to drive innovation, enhance operational efficiency, and accelerate your digital transformation journey.

Security and Privacy Measures in VIVE Intelligent Device Series

In today's rapidly evolving digital landscape, privacy and security are paramount, especially for businesses leveraging virtual and augmented reality technologies. VIVE understands these concerns and has developed a comprehensive security framework to safeguard sensitive information and ensure reliable user experience. VIVE Intelligent Devices prioritize user privacy by processing and storing data locally. Privacy protection is strengthened by promoting transparency in data handling and user consent. To enhance transparency, recording or taking screenshots is only possible when the user has enabled the feature in passthrough mode, and an LED indicator light on the front of the device will illuminate to signal that recording is active.

Secure Operating System

VIVE's operating system is built upon the Android Open Source Project (AOSP), inheriting its core architecture and security features. By leveraging the mature and well-maintained security mechanisms of the Android platform, VIVE ensures a trusted and resilient foundation for its devices.

These features can make your VIVE devices as secure as possible:

Application Sandbox

The Android platform leverages Linux's user-based protection mechanisms to identify and isolate application resources. Each Android app is assigned a unique user ID (UID) and runs in its own process. This UID is then used by the system to create a kernel-level Application Sandbox, ensuring process and data isolation.

App Signing

App signing allows developers to identify the author of the app and to update their app without creating complicated interfaces and permissions. Every app that runs on the Android platform must be signed by the developer.

Authentication

Android uses the concept of user-authentication-gated cryptographic keys that require cryptographic key storage and service provider and user authenticators.

Encryption

Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk and all reads automatically decrypt data before returning it to the calling process. Encryption ensures that even if an unauthorized party tries to access the data, they can't read it.

Keystore

Android offers a hardware-backed Keystore that provides key generation, import and export of asymmetric keys, import of raw symmetric keys, asymmetric encryption and decryption with appropriate padding modes, and more.

Security-Enhanced Linux

As part of the Android security model, Android uses Security-Enhanced Linux (SELinux) to enforce mandatory access control (MAC) over all processes, even processes running with root or superuser privileges (Linux capabilities).

Trusty Trusted Execution Environment (TEE)

Trusty is a secure Operating System (OS) that provides a Trusted Execution Environment (TEE) for Android. The Trusty OS runs on the same processor as the Android OS, but Trusty is isolated from the rest of the system by both hardware and software.

Verified Boot

Verified Boot strives to ensure all executed code comes from a trusted source (usually device OEMs), rather than from an attacker or corruption. It establishes a full chain of trust, starting from a hardware-protected root of trust to the bootloader, to the boot partition and other verified partitions.

Hardware and Firmware Security

eFuse (electronic fuse)

A hardware protection mechanism used in electronic devices to prevent unauthorized modifications or tampering at the hardware level.

Firmware and OS Security Updates Mechanism

Ensures the integrity of the software through verified boot processes and provides regular firmware and OS security updates to protect against vulnerabilities and maintain system trustworthiness.

Device Access Control

Enforce the use of a PIN, password, pattern, or device passcode to strengthen user authentication and protect access to the device.

Trusted Execution Environment

Provides a secure enclave for sensitive operations, protecting data from software-based attacks.

Access Indicators

Visual indicators notify users whenever applications access sensitive hardware components such as the microphone or camera. This transparency measure helps users maintain awareness and control over their device privacy.

Privacy Dashboard

Allows users to manage app permissions and data access.

Network Security

VIVE Intelligent Devices are designed with robust wireless security features, ensuring secure and reliable connections across various environments. Our devices support advanced Wi-Fi security protocols that provide protection for both personal and enterprise use:

- Enhanced Protection for Personal and Enterprise Networks: Supports strong encryption and authentication standards, safeguarding wireless communication against unauthorized access and known vulnerabilities
- Secure Connectivity for Public Networks: Enables secure encryption for open Wi-Fi environments, ensuring user privacy even on shared or public hotspots.
- Certificate-based Authentication: Incorporates high-assurance authentication mechanisms, including certificate-based methods, to deliver the highest level of network security for sensitive environments.
- Alignment with Industry Standards: All wireless security measures align with current Wi-Fi security best practices to ensure ongoing protection against emerging threats.

Data Transmission with Encryption

The VIVE Operating System is designed to prioritize data protection during transmission, implementing multiple layers of safeguards to ensure secure communication:

- Blocking Cleartext Traffic: By default, the system prevents unencrypted (cleartext) data transmission, ensuring that sensitive information is always sent securely.
- Enforcing Strong Encryption Standards: Data exchanged between VIVE Intelligent Devices and servers is protected using advanced encryption protocols, ensuring confidentiality and integrity throughout the transmission process.
- Multi-layered Security Approach: The platform leverages diverse network security measures, integrating multiple encryption and authentication mechanisms to provide comprehensive protection for data in transit.

Data Encryption-At-Rest

VIVE Intelligent Devices safeguard user data with strong encryption methods that ensure information remains protected while stored on the device. The platform employs file-based encryption, where individual files are encrypted with unique keys securely managed within a trusted environment, providing granular control and robust protection against unauthorized access.

Application Security

VIVE ensures a safe app ecosystem through a rigorous review process:

- Principle of Least Privilege and App Permissions

  Apps should only have the minimum permissions necessary to perform their functions.
- Scoped Storage

  Restrict each app to accessing only its own private data, while access to shared storage areas (such as photos, music, and documents) requires user permission or must be done through official APIs.

Privacy Features

All VIVE Intelligence Devices share several privacy and security features, ensuring robust protection for users. Key features include:

- Permission Control: Provides visibility and control of permissions that installed apps are currently using.
- User Data Collection Transparency: Understand the types of information collected.
- Camera and Mic Auto Sleep: Automatically disables the VIVE device cameras and microphones when the VIVE device enters sleep mode, reactivating them only when the power button is pressed.

Mixed Reality and Camera Data

Some VIVE Intelligence Devices enable mixed reality (MR) applications, which allows users to enhance their surroundings with interaction of both virtual and real-world environments. These experiences leverage spatial data collected by the camera on the VIVE Intelligent Devices, empowering VIVE devices and apps to deliver unique and sophisticated MR functionalities.

Cameras in VIVE Intelligence Devices capture and process image data locally on the device. This ensures that sensitive information remains private and is not shared with HTC or any third parties. By keeping camera data processing on-device, HTC enhances user privacy without compromising the quality of mixed reality experiences.

HTC is committed to minimizing data collection and sharing. Only the essential data required for the operation, improvement, and security of VIVE Intelligence Devices is collected and processed. No camera data or spatial data is transmitted to HTC, and HTC neither requests nor requires the sharing of any additional data for commercial purposes. By processing camera data locally on the device, HTC ensures that user privacy is prioritized and that sensitive information remains protected. This approach reflects HTC's ongoing dedication to safeguarding user information throughout every stage of the product lifecycle.

VIVE VR Accessories

The VIVE Intelligent Device Series offers a range of accessories that enhance the functionality and comfort of your VIVE Intelligent Devices, delivering a more immersive virtual reality experience.

VIVE Ultimate Tracker is compact, versatile, and featuring two wide-field-of-view (FOV) cameras with self-tracking technology that operates without the need for base stations. It is ideal for standalone VIVE Intelligent Devices and support for both OpenXR and SteamVR on PC. It uses a standard 1/4”-20 UNC mount and pogo pin interface for easy attachment to various objects, enabling use cases like motion capture, VR training, and full-body tracking in apps like VRChat. Developer resources, including documentation and 3D CAD files, are also available for custom mount designs.

VIVE Wrist Tracker is a wearable device for precise wrist and hand tracking. Using high-frequency IMU (Inertial Measurement Unit) data and kinematic models, it accurately predicts motion even out of view, ensuring low-latency, real-time tracking in VR.

VIVE Full Face Tracker is a plug-and-play USB-C module that enables detailed face and eye tracking on compatible devices. It captures 38 facial blend shapes at 60 Hz and tracks eye movements at 120 Hz, allowing for natural expressions and real-time lip-sync. It also auto-calibrates Interpupillary Distance (IPD) for optimal comfort and clarity.

Our Meticulously Crafted Security Controls

Wireless Communication Security

VIVE Ultimate Tracker and VIVE Wrist Tracker utilize VIVE's proprietary wireless communication protocol, which offers enhanced security protection compared to standard wireless technologies. This ensures that communication between devices remains private and secure.

Data Transmission Security

All data transmitted by the VIVE Ultimate Tracker and VIVE Wrist Tracker is protected with strong encryption standards, maintaining confidentiality and integrity throughout the transmission process. This ensures sensitive information is secure at every step of communication.

Tracker and Device Authentication

VIVE Ultimate Tracker and VIVE Wrist Tracker incorporate robust authentication measures during the pairing process, including the generation of random numbers and identity verification mechanisms. This establishes a trusted and secure connection between devices. Upon successful pairing, visual feedback via the user interface and LED indicators confirms connection status, ensuring transparency for users.

Firmware Integrity Verification

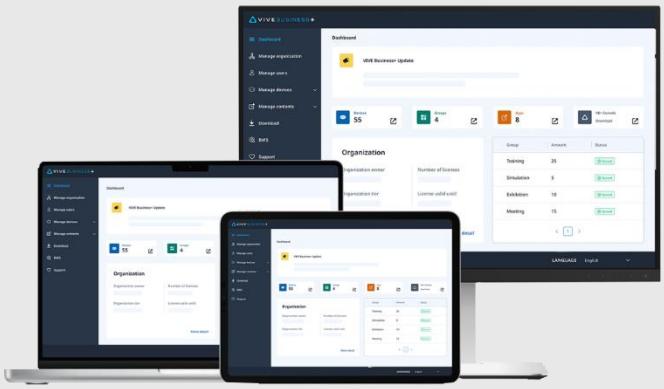
The VIVE Ultimate Tracker employs firmware integrity verification mechanisms to ensure that all firmware components are cryptographically validated throughout the boot process. This verification occurs from the initial power-on through to full system launch, protecting the device against unauthorized firmware modifications.

Secure Firmware Updates

To maintain system integrity and address potential security vulnerabilities, the VIVE Ultimate Tracker supports secure over-the-air (OTA) firmware updates. All update packages are digitally signed and verified, ensuring that only authenticated and authorized firmware is installed on the device.

VIVE Device Management Platform

VIVE Business+ is a cloud-based platform designed to support organizations in managing and securing virtual reality (VR) and mixed reality (MR) devices across diverse environments. The platform offers a comprehensive set of features, including remote device monitoring, content management, and customizable user interfaces, all while maintaining a strong commitment to data security and privacy. Built on a scalable serverless architecture hosted by Amazon Web Services (AWS), VIVE Business+ is designed with security and privacy as core principles. By implementing industry best practices in line with internationally recognized standards, the platform ensures that customer data remains secure and protected throughout its lifecycle.



Key security measures include robust data encryption, stringent access controls, and a clear emphasis on customer data ownership. Regular security audits and vulnerability assessments are conducted to ensure the platform's ongoing resilience and reliability. VIVE Business+ is particularly suited for organizations that require centralized management of multiple Intelligent Devices and trackers, serving industries such as enterprises, educational, and healthcare to enable efficient secure operation of VR and MR experiences.

By streamlining VR operations through a secure, intuitive platform, VIVE Business+ empowers organizations to focus on delivering impactful, immersive experiences while maintaining high standards of operational security and device governance.

Key Features

Device Management

VIVE Business+ offers management controls and security features to help organizations adopt VIVE Intelligent Devices and trackers.

- **Device Management**: VIVE Business+ enables quick device enrollment, remote management, and configuration updates. VIVE Intelligent Devices can be seamlessly enrolled through QR code scanning or USB connections.
- **Group Management**: Devices can be organized into groups to streamline updates and settings deployment. Admins can also create private groups to manage access more efficiently.
- **Remote Monitoring**: Admins can remotely monitor device status, battery levels, and Wi-Fi status. Devices can also be remotely rebooted, shut down, or factory reset.
- **User Management**: VIVE Business+ enables adding users and assigning roles (admin, operator, member). Multiple organizations can be created for separate teams.
- **Batch Configuration**: Customizable settings can be applied across groups of VIVE Intelligent Devices

Content Management

- **Content Library**: Upload and manage apps, maps, and media files in the cloud. Supported file types include .apk, .obb, images, audio, and videos.
- **Content Deployment**: Distribute apps and updates to individual VIVE Intelligent Devices or groups remotely. Content can be launched, or events can be triggered in real time.

Advanced Customization and Control

- **Customized User Experience**: Deliver a branded user experience by customizing the startup logo and animation, as well as system functions and user interfaces.
- **Kiosk Mode**: Lock users into specific experiences by customizing app permissions, network security, and more.
- **Visual Odometry (VO) Mode**: Bypass environment setup for faster deployment across various environments.
- **API Access**: Enables powerful, granular customization and integration with platform and device-level API access.

Online and Offline Versatility

- **Online Web Application**: Manage devices and content via the VIVE Business+ web application.
- **Offline Operations**: Use the VIVE Business+ Console for core features with limited or no internet access.

Tracker Management

- **VIVE Ultimate Tracker Management**: Manage and deploy VIVE Ultimate Trackers alongside VIVE Intelligent Devices. Access tracker-specific features for seamless deployments.

Location-Based Entertainment (LBE) Mode

- **Large-Scale Tracking Support**
  - Supports tracking areas up to 1,000 m².
  - Uses inside-out 6DoF tracking (no external sensors needed).
- **Custom Map Creation & Persistent Relocation**
  - Supports irregular play area boundaries (L-shaped, polygonal, etc.).
  - Devices automatically relocate when re-entering the space—no need to return to the origin.
- **Multi-Device, Multi-User Support**
  - Multiple standalone headsets (e.g., VIVE Focus 3, XR Elite) can operate simultaneously in the same space.
  - Enables synchronized multiplayer VR experiences.
- **Marker-Based Tracking Enhancements**
  - Marker-Based Drift Prevention: Prevents positional drift over time.
  - Marker-Based Advanced Relocation: Enables relocation from any spot within the space.
  - Marker-Based Scene Alignment: Aligns virtual content with physical layout precisely.
- **LBE Hybrid Mode**
  - Seamlessly transitions between Visual Odometry (VO) and LBE modes.
  - Ideal for experiences where users move from setup/waiting area to gameplay zone.
- **Multiple Tracking Modes**
  - VO Mode: Fast deployment, no map creation needed.
  - 3DoF Mode: Tracks rotation only.
  - Passenger Mode: Tracks only rotation using IMU; ideal for motion-based settings.
  - Simulator VR Mode: Designed for use with racing/flight simulators, seats, and steering devices.
  -

- **Wi-Fi LBE Mode (for VIVE Ultimate Tracker)**
  - Utilizes Wi-Fi to connect trackers directly to the headset.
  - Eliminates the need for dongles or cables.
  - Enhances deployment efficiency in commercial venues.
- **Centralized Management via VIVE Business+**
  - Supports batch setup and remote deployment.
  - Manages devices, content, and maps through a single interface.
  - Optimized for commercial operators.

Security and Privacy Measures in VIVE Business+

Secure Architecture and Device Registration

VIVE Business+ is built on a secure architecture that manages XR devices via strict registration mechanisms. Each device is assigned a unique credential to ensure that only authorized hardware can access the platform, thereby preventing unauthorized access and maintaining comprehensive oversight of all managed devices.

Data Encryption and Protection

All data transmitted through the VIVE Business+ Console is secured using advanced encryption protocols, ensuring confidentiality and integrity during transfer. Data stored in the cloud and on devices is protected by robust encryption methods compliant with industry-recognized security standards. Sensitive configuration files and assets are safeguarded through multi-layered encryption techniques.

Network Defense Mechanisms

The platform incorporates multiple layers of network protection, including firewalls, application-level security, and distributed denial-of-service (DDoS) mitigation. Communication between devices and the console is secured through encrypted channels, ensuring data integrity and confidentiality throughout the transmission process.

Access Control and Authentication

Role-based access control (RBAC) and multi-factor authentication (MFA) are implemented to ensure that only authorized personnel can access sensitive organizational data. Logical access to systems and data is periodically reviewed to maintain data confidentiality and prevent unauthorized access. VIVE Business+ also supports two-factor authentication (2FA) for additional security during user logins.

Serverless and Scalable Architecture

VIVE Business+ operates on a secure, serverless cloud infrastructure based on industry-leading cloud services. This architecture reduces risks associated with physical servers and enables automatic scalability. Physical security is maintained in accordance with rigorous third-party audit standards.

Multi-Layered Security Framework

A comprehensive, multi-layered security approach is employed across application security, data encryption, and cloud infrastructure. These layers collectively ensure that organizational data remains protected throughout the entire device management lifecycle.

Cloud Certifications and Compliance

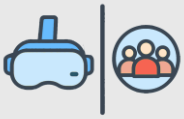
VIVE Business+ is hosted on a trusted cloud infrastructure that complies with internationally recognized security and privacy standards.

Personnel Security and Governance

All personnel with access to sensitive systems and data are required to adhere to strict security protocols, undergo regular security training, and operate under the Principle of Least Privilege. Activity monitoring ensures continuous oversight and accountability.

Logical Separation

VIVE Business+ ensures the logical separation of customer data through organizational IDs. Each user's data is isolated to prevent access by other organizations.



Device-Group Management

VIVE Business+ organizes VIVE Intelligence Devices into groups, enabling efficient batch configuration. This structure allows seamless access to curated apps across all devices within a group, ensuring a consistent user experience and compliance with organizational policies.

Forced Login for Individual Control

VIVE Business+ enforces user authentication at the device level, ensuring that only designated organizational accounts are used. This approach prevents the use of personal accounts and helps maintain organizational control.

VIVE Business+ is built with a strong commitment to transparency, robust security controls, and strict adherence to data protection standards. The platform prioritizes customer data ownership, ensuring that customer data is never used for advertising purposes nor shared with third parties without explicit consent. Through a comprehensive security framework and continuous privacy-first practices, VIVE Business+ empowers organizations to manage devices with confidence, safeguarding sensitive information at every stage.

VIVE PC VR Streaming Service

VIVE Streaming enables seamless, high-quality content streaming across multiple endpoints, delivering immersive gameplay and large-scale visual presentations with consistently low latency and high visual accuracy. Designed to enhance user experience without compromising performance, it extends the capabilities of VIVE Intelligent Devices in both consumer and enterprise environments.

Security and privacy are fundamental to the design of VIVE Streaming. A two- tier encryption framework protects video and audio streams. During session initialization, strong public key encryption is applied to securely exchange session keys. Once the session is established, proprietary encryption techniques are used to protect the data stream, ensuring continuous confidentiality and integrity. This layered encryption approach provides comprehensive protection across the entire streaming session.

For enterprise deployments, the VIVE Streaming client application further verifies device configurations, ensuring that only those provisioned and authenticated through VIVE Business+ management policies are accepted. This prevents unauthorized configurations and ensures organizational security standards.

VIVE Streaming is designed with privacy at its core. All video and audio streaming occurs locally between the VR device and the PC through a secure local network. No streaming data is transmitted to HTC or to any cloud servers. This ensures that users retain complete control over their content and that no external entities have access to the streamed data.

VIVE VR Workspace Service

VIVE Desk is a virtual reality (VR) application that allows users to extend their Windows or macOS desktop into immersive virtual spaces. It is designed to enhance productivity through multi-monitor support, intuitive interaction, and immersive workspace customization. The application is deployed locally on the user's VIVE Intelligent Device and connects to the user's computer via a secure local connection.

Key Features

- **Multi-Monitor Display**: Up to three configurable virtual monitors to extend desktop space within VR.
- **Mixed Reality Mode**: With MR features, you can see your hands, mouse, and keyboard in the virtual environment, enabling intuitive and precise input while maintaining awareness of your surroundings for safety.
- **Customizable Workspace**: Adjustable the screen size and positions, including ultra-wide modes for media or multitasking.
- **Immersive Environments**: Work in a variety of VR environments or dim your physical surroundings in MR mode to reduce distractions and improve concentration.
- **Portable Office Experience**: No traditional desk required. Simply connect to the VIVE Intelligent Devices with controllers or Bluetooth devices for a flexible and comfortable setup, perfect for work or leisure anywhere.

With VIVE Desk, you can create a flexible and efficient hybrid workspace that merges the physical and virtual worlds. Whether you're managing work tasks or enjoying entertainment, it breaks physical limitations and delivers an entirely new immersive experience. Featuring multitasking capabilities, virtual screen control, and intuitive data management, VIVE Desk enhances focus and productivity in both virtual and mixed reality environments.

Security and Privacy Measures in VIVE Desk

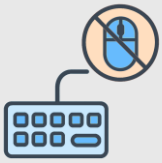
VIVE Desk is designed with local processing in mind. All screen content rendered in VR originates from the user's computer and is streamed over a secure, local network connection. No screen data, user input, or usage activity is transmitted to HTC servers or external cloud infrastructure.

Local-Only Data Handling

The application does not upload or sync user screen content to HTC or third-party services.

No Persistent Storage

VIVE Desk does not store sensitive user data on the device or in the cloud.



Input Privacy

All keyboard and mouse input occurs locally and is not logged, recorded, or transmitted.

User-Controlled Environment

Users fully control workspace layout, session initiation, and the presence of MR elements.

This security- and privacy-by-design approach ensures that users retain full control over their content and interactions within VIVE Desk. It reflects HTC's broader commitment to secure-by-default architecture and privacy-centric immersive technology.

VIVE Education Management Platform

VIVE Host is an XR (Extended Reality) device and content management platform designed to streamline the deployment and oversight of VIVE Intelligent Devices across classrooms, training centers, and business environments. It enables the seamless delivery and management of VR, MR, and multimedia content directly to devices without the need for a PC, operating instead through a tablet running iOS or Android.

Key Features

- **Easy Setup**: Devices can be quickly registered to VIVE Host by simply scanning a QR code, making setup fast and effortless.
- **Device Monitoring and Control**: Check the battery level, device settings, and currently running or installed content. You can even shut down or restart VIVE Intelligent Devices remotely from the tablet.
- **Wide Content Support**: Install, manage, and launch content across all VIVE Intelligent Devices with a single click. VIVE Host supports VR and MR experiences, 360° videos, WebXR, images, audio files, standard videos, and webpages, making it ideal for a variety of training and educational applications.
- **Flexible Control Modes**: Choose between two modes. Free Mode allows users to explore content at their own pace, while Broadcast Mode provides instructors or facilitators with full control over the content being delivered, making it ideal for guided lessons or demonstrations.
- **Real-Time Monitoring and Interaction**: Mirror VIVE Intelligent Devices screens to VIVE Host so you can view exactly what each user sees. Monitor multiple screens at once and communicate with users in real time, which enhances both learning and engagement.
- **Usage Analytics**: Access usage history and analytics right from the dashboard to better understand how content is being used and to refine your programs accordingly.

VIVE Host offers a powerful, user-friendly solution for managing XR content and devices in multi-user environments. It's designed to elevate the immersive learning and training experience through smart, centralized control.

Security and Privacy Measures in VIVE Host

Serverless and Multi-layered Security Framework

Built on a secure, serverless cloud infrastructure, the platform employs a multi-layered security framework across applications, data encryption, and cloud services. Ensuring end-to-end protection of organizational data throughout the lifecycle.

Secure Communication Protocols

All platform communications are secured through advanced encryption protocols that support a range of modern cryptographic algorithms. These protocols ensure data confidentiality, integrity, and authentication, and are periodically reviewed to maintain alignment with current security standards.

Secure Design

During the design phase, the platform undergoes thorough threat analysis using threat modeling tools to proactively identify and address potential threats.

Vulnerability Management

Regular source code scanning and mobile application security testing are conducted to ensure a comprehensive security posture and enable proactive threat mitigation.

Risk Assessment and Management

- The platform team conducts routine risk assessments and maintains an up-to-date inventory of information assets to identify potential threats.
- Mitigation strategies are proactively implemented to minimize the risk of security breaches or operational disruptions.

Disaster Recovery and Business Continuity

- Resilient infrastructure support ensures continuous service availability during regional outages or disruptions.
- Backup mechanisms and routine disaster recovery drills help maintain operational continuity and reduce the impact of unforeseen incidents.

VIVE Mars CamTrack

A Professional Camera Tracking Solution Designed for Virtual Production

VIVE Mars CamTrack is a professional virtual production solution, designed to seamlessly integrate real-world camera footage with virtual environments. It empowers content creators across film, broadcast, and live production industries by streamlining workflows and enabling greater creative flexibility. Leveraging VIVE Tracker 3.0, SteamVR Base Stations, and HTC's proprietary Mars system, VIVE Mars CamTrack delivers a plug-and-play camera tracking experience that significantly reduces the technical complexity and setup time typically associated with virtual production environments.

Key Features

- **Multi-Camera Tracking Support**: Enables real-time tracking for up to three cameras simultaneously, supporting dynamic multi-angle virtual production.
- **High-Precision, Low-Latency Tracking**: Powered by VIVE Tracker and the SteamVR tracking system, delivering accurate and responsive positioning data with minimal latency.
- **Genlock and Timecode Synchronization**: Built-in support ensures frame-accurate synchronization between physical and virtual footage, minimizing latency and visual drift.
- **Streamlined Setup, Fast Deployment**: User-friendly configuration allows small teams or individual creators to deploy systems rapidly with no complex setup required.
- **Native Integration with Unreal Engine**: Provides seamless compatibility with Unreal Engine, supporting LED walls and green screen workflows across diverse production scenarios.

VIVE Mars CamTrack high-quality virtual production more accessible, efficient, and scalable, making it Ideal for film studios, commercial production teams, broadcast environments, and educational institutions.

Security Measures in VIVE Mars CamTrack

All firmware and control software associated with VIVE Mars CamTrack are developed and distributed exclusively by HTC VIVE. To maintain system integrity and resilience:

Secure Update Mechanisms

Firmware and software updates are delivered through secure channels with version control and rollback capabilities.

Local Data Processing

All tracking data is processed within the local production environment and is managed through Unreal Engine without transmission to HTC or any external servers.

Software Authenticity

All drivers, plugins, and system binaries are digitally signed to verify authenticity and protect against unauthorized modifications.

Security Testing

Regular security testing, including compatibility and stability assessments with Unreal Engine, is conducted to ensure robust integration and operational security.

Security Best Practices

- Operate all Mars CamTrack components on a closed local network (no internet exposure).
- Employ VLANs or physical network segmentation between Mars CamTrack and other production systems.
- Keep all Trackers and firmware up to date with the latest official releases.
- Follow Epic Games' Unreal Engine security best practices for project development and deployment.

By combining strong local-only processing, proactive software security, and robust deployment practices, VIVE Mars CamTrack supports secure, scalable, and reliable virtual production environments aligned with modern enterprise security expectations.

5G Private Network System

Trends and Enterprise Applications of 5G Private Networks

With the rise of digital transformation and smart applications, enterprises increasingly demand dedicated communication networks with high bandwidth, low latency, and strong controllability. The 5G Private Network (Private 5G Network) has emerged to meet these needs, offering a dedicated, isolated, and manageable mobile communication environment for enterprises or specific sites. It is widely applied in areas such as smart manufacturing, smart healthcare, remote education, smart logistics, and immersive XR experiences.

Positioning and Core Advantages of 5G Private Networks

G REIGNS specializes in 5G core communication technologies, with a focus on developing Baseband Units (BBUs) based on the O-RAN architecture. By deeply integrating VR technologies, we support a wide range of application scenarios, including training, exhibitions, and development. Our solution delivers a flexible, modular, and technically advanced 5G private network that is compact yet powerful.

Additionally, our company integrates radio units (RUs), 5G core networks (5GC), and other 5G technologies, offering highly portable core advantages, including:

- Strong Independent Development Capability

  Mastery of BBU key technologies, enabling deep customization and rapid deployment.
- Support for Emerging Application Integration

  Seamless integration with VR/MR devices and trackers to create low-latency immersive experiences.
- Highly Flexible Design

  Supports diverse site architectures and topology requirements, adaptable to various industry scales.
- Agile Technical Support

  A small, agile team capable of quickly responding to market and customer needs.
- High Portability

  Development of highly integrated products, providing 5G networking convenience within a carry-on suitcase.
- Integration

  Compatibility with RUs and 5GC developed by other vendors.

Why Security is Critical to 5G Private Networks

The openness and programmability of 5G private networks enhance deployment flexibility and efficiency but also introduce new security risks. A successful attack could lead to production line disruptions, data breaches, or service paralysis. Therefore, establishing a trustworthy security framework and implementing zero-trust principles are primary considerations for enterprises adopting 5G private networks.

Security Challenges of 5G Private Networks

The deployment of 5G private networks faces the following security challenges:

- Network Attack Risks

  The open architecture of 5G (e.g., Open RAN) may increase vulnerabilities from unverified devices.
- Device Proliferation

  The growing number of IoT devices introduces more potential entry points for attacks.
- Data Privacy

  Large-scale transmission of sensitive data requires protection against theft or tampering.
- Supply Chain Risks

  Complex hardware and software sources may conceal backdoors.
- Latent Threats

  Malicious programs (e.g., Trojans) may remain dormant for extended periods, evading detection.
- Uncontrolled IoT Device Access

  Unauthorized devices could serve as steppingstones for intrusions.

Security Features and Management Measures Provided by G REIGNS's 5G Private Network Equipment

We integrate advanced technologies and practical features to address the security challenges of P5G with the following strategies:

Signaling Encryption and Integrity Protection

Employs NAS/AS layer encryption to prevent eavesdropping or tampering with content.

User Identity Verification and Device Authentication

Supports SIM-based authentication and remote attestation mechanisms.

Control Plane and User Plane Entity Isolation

C-Plane and U-Plane entities are physically separated, ensuring traffic isolation and preventing user data from accessing management ports.

End-to-End Logging and Monitoring

Provides comprehensive logging information, including unauthorized access attempts, with the ability to transmit data to external archives for enhanced threat visibility.

SIM and Device Binding

Prevents SIM reuse or theft on unauthorized devices, with immediate system notifications and registration blocking in case of misuse.

System Design Protection

Adopts minimal access principles and layered authorization to reduce vulnerabilities.

SBOM

Implements Software Bill of Materials (SBOM) reviews for third-party vendors and manages risks using Common Vulnerability Scoring System (CVE/CVSS).

Enterprise Private Network Site Security Recommendations

As an O-RAN telecommunications equipment provider, our 5G Private network products include built-in security features that offer foundational protection for P5G networks. However, the security of the product itself is only one piece of the overall security puzzle. When deployed in real-world sites, the site-specific security controls, management measures, and architectural design determine the overall security strength. Below are recommended security measures to maximize the protection of P5G networks at the site level.

Layered Security Architecture Design

Site security requires a Defense-in-Depth strategy to ensure subsequent layers of protection remain intact if one layer is breached. Recommended measures include:

- **Edge Layer Protection**: Deploy advanced firewalls and intrusion detection systems (IPS/IDS) at the site edge to filter external threats and restrict unauthorized access.
- **Core Layer Isolation**: Use network segmentation technologies (e.g., VLAN or physical isolation) to separate critical business traffic from general traffic, reducing lateral spread risks.
- **Application Layer Monitoring**: Perform behavioral analysis on applications within the site to detect anomalies and prevent data leaks.

  This multi-layered architecture ensures that even if one segment is compromised, attackers face multiple barriers, significantly enhancing overall protection.

Implementation of a Centralized Security Operations Center (SOC)

Site owners can deploy an integrated Security Operations Center (SOC) to achieve comprehensive threat management. Core SOC functions include:

- **Monitoring**: Integrates monitoring data provided by 5G Private Network System to analyze behavioral patterns of network traffic on N6/N3 interfaces within the site.
- **Incident Response**: When potential threats are detected, the SOC can quickly initiate response procedures, such as isolating affected devices or blocking malicious traffic.
- **Log Analysis and Traceability**: Centrally collects and analyzes site logs to support post-incident investigations and regulatory compliance.

High Availability (HA) Design

The high availability of our 5G Private network system is critical not only for business continuity but also for security. Sites can adopt an HA architecture for P5G network deployment.

Site Control Measures

In addition to technical architecture, site-specific control measures are equally important:

Access Control Management:

- Implement the Principle of Least Privilege to ensure employees and devices only access necessary resources.
- Physical Security: Protect physical equipment within the site (e.g., base stations and servers) to prevent unauthorized access or tampering.

We provide foundational security features, but the deployment architecture and management strategies at the site level are the final mile in achieving comprehensive security. Enterprises should tailor security solutions based on site characteristics (e.g., scale, industry needs) to ensure seamless integration of product features with site measures. Only by combining product-level protection with site-level controls can an impregnable P5G security framework be established.

Security Compliance and Standards

G REIGNS's 5G private network system products have passed multiple international and local standard verifications, ensuring compliance with global and regional security requirements. Our solutions not only help enterprises mitigate threats but also excel in security audits and regulatory compliance, strengthening market competitiveness.

International Standard Certification

Our P5G network products have met partial test requirements of the Third Generation Partnership Project (3GPP) security specifications, including:

3GPP TS 33.511

Security controls and testing specifications for 5G base stations (gNodeB), ensuring security and reliability in network deployment.

3GPP TS 33.117

Covers general security requirements, including vulnerability scanning and penetration testing, validating compliance in access control and data protection.

3GPP TS 33.210

Focuses on network-level security mechanisms to ensure encryption and integrity of data transmission.

These tests were conducted by the internationally recognized Open Testing and Integration Centre (OTIC) laboratory, with official 3GPP test reports obtained, confirming that our BBU products meet industry standards in key security areas.

In addition to 3GPP-related security specifications, G REIGNS products comply with the security requirements established by the O-RAN Alliance's Security Working Group, ensuring robust protection for our BBU products in open radio access network environments. These requirements encompass device authentication, interface encryption, and vulnerability management, further enhancing the security and interoperability of our products in multi-vendor ecosystems.

Moreover, the P5G network system participates in the Telecom Infra Project (TIP) testing and certification programs, successfully passing TIP's interoperability and security tests for open network equipment. Our products adhere to TIP's security best practices, ensuring stable operations and data protection in open architecture.

Local Regulatory Compliance in Taiwan

In the Taiwan market, G REIGNS's P5G network system has passed the testing requirements of the Fifth Generation Mobile Communication Base Station Security Inspection Guidelines established by the National Communications Commission (NCC). This guideline imposes strict standards on 5G private network equipment security, covering device authentication, network protection, and vulnerability management. Our products have successfully obtained NCC-approved test reports, ensuring compliance with local regulations and meeting enterprise customers' compliance needs.

From device authentication and signal encryption to network isolation, we deliver a multi-layered defense system designed to safeguard every corner of your communication infrastructure. We adhere to global security standards and reinforce our commitment through regular audits and rigorous testing. Looking ahead, G REIGNS continues to invest in next-generation security technologies, empowering enterprises with a reliable, future-ready 5G platform built for performance, protection, and peace of mind.

Furthermore, G REIGNS's P5G network system products meet the security testing standards set by major Taiwanese telecommunications operators, as well as the stringent security requirements of government procurement projects.

VIVE ORIGINALS

VIVE ORIGINALS focuses on the development and distribution of original extended reality (XR) content. It integrates a range of emerging technologies, including volumetric capture, blockchain, and XR, to support innovation in storytelling across film, arts, music, and immersive media applications in the metaverse.

One of its signature productions, BEATDAY, exemplifies this innovation. BEATDAY is a music-focused metaverse ecosystem that enables audiences to experience real-time virtual performances and explore digital environments enhanced by blockchain-enabled asset interaction. It reflects HTC's vision for interactive, immersive Web 3.0 experiences.

All content development under VIVE ORIGINALS follows HTC's secure content production standards. Industry-aligned data security practices govern user identity, interaction data, and the handling of digital assets. Through VIVE ORIGINALS, HTC promotes cross-sector creative exploration while maintaining a responsible and security-conscious approach to immersive media.

VIVE ORIGINALS upholds a creative philosophy that blends cultural innovation with cutting-edge immersive technologies. Through collaborations with visionary artists and storytellers, it explores new dimensions in interactive experiences, immersive performance, and audience co-creation. Each production is designed not only as content, but as a cultural dialogue—bridging virtual worlds with real-world emotional resonance.

Beatday — Virtual Entertainment Brand

Beatday is a cutting-edge holographic entertainment platform developed by HTC VIVE ORIGINALS. It integrates XR, volumetric capture, motion tracking, and 3D animation technologies to deliver an unprecedented interactive virtual experience. On the BEATDAY platform, users can participate in live performances, whether by real-life or virtual artists, through their PC or VR devices using customizable avatars and full 6DoF (six degrees of freedom) viewing, redefining the traditional way of enjoying entertainment and creating an unparalleled "ultimate front-row" experience.

The Beatday client application is built on the Unity engine and supports multiplayer interactions, player data management, and asset visualization. Performance content is dynamically updated based on the specific event being presented.

The backend is built on a scalable cloud infrastructure, leveraging cloud-native services for content delivery, data processing, and multiplayer synchronization. The architecture supports efficient communication between client applications and backend services, ensuring seamless user experiences during performances and interactions.

In designing the system architecture, BEATDAY follows key security principles to ensure overall system security and stability.

Security and Privacy Measures in Beatday

Data Handling and Transmission

- User data is processed and stored via a secure, scalable cloud infrastructure aligned with international security and privacy standards.
- All communication between clients and backend services is encrypted using protocols that protect the confidentiality and integrity of transmitted data.
- Data Sensitivity: Sensitive transaction-related information is handled with appropriate safeguards and design practices aligned with modern application development to prevent unauthorized access.

Network Security

- The system operates within a logically segmented virtual cloud environment that distinguishes between public-facing and internal services.
- Network communication is governed by predefined access control policies that enforce strict traffic rules between services. Combined with application-layer protective mechanisms, the system is resilient against Distributed Denial of Service (DDoS) attacks and ensures that service interactions operate within expected boundaries.
- Scalable strategies are applied to manage traffic surges, providing smooth and reliable service availability.

Access and Interaction Control

- User sessions are managed with token-based mechanisms that facilitate secure and flexible user interactions.
- Role-based access control is implemented across the platform to enforce the Principle of Least Privilege and ensure proper access segregation.

Monitoring and Operational Oversight

- The platform integrates monitoring tools and anonymized telemetry to detect anomalies and optimize performance.
- Alerts and monitoring tools help identify operational anomalies, ensuring timely support and issue resolution.
- Access to operational logs and diagnostic data is limited to authorized personnel and subject to internal review.

Through these layered security measures and architectural controls, BEATDAY delivers an innovative and immersive entertainment experience while maintaining highest standards for data protection, system integrity, and operational reliability.

VR Theatre Management System

A dedicated system for synchronized multi-user playback and management of VR experiences in theaters

The VR Theatre Management System is an all-in-one VR screening solution for film festivals, immersive exhibitions, and location-based entertainment venues. This system brings creators and audiences together in a shared virtual cinema experience that is highly scalable, deeply immersive, and effortlessly synchronized across multiple viewers.

Key Features

- **Synchronized Playback System**: One-click multi-user synchronized playback, ideal for large-scale venues and special showcase events.
- **Centralized Control App**: Content scheduling, automated playback, and remote system monitoring help significantly reduce manpower requirements.
- **Modular Deployment**: Flexible installation to fit various venue sizes and use cases from temporary exhibitions to long-term commercial cinemas.

We recognize that content integrity and audience privacy are critical to the future of immersive media. The VR TMS is built with robust security protocols across content distribution, playback authorization, and system communication, ensuring confidentiality, integrity, and availability at every stage.

Security and Privacy Measures in VR Theatre Management System

Content Protection and Licensing Control

- Adopts the Digital Cinema Package standard for encrypted media distribution and playback authorization.
- Supports Key Management Systems in restricting content access to authorized venues and timeframes.
- Optional forensic watermarking and digital fingerprinting to prevent unauthorized duplication or leaks.

Secure Centralized Management

- Authorized device login only; all operations are logged for audit purposes.
- Role-based access control (RBAC) is used to limit exposure to human error or insider threats.

Device and Network Security

Option to deploy in offline or local area network (LAN) environments, no internet required for playback.

DeepQ

In a future where technology drives the evolution of healthcare, DeepQ plays a pivotal role in leading the transformation toward smart, connected medicine. Since its founding in 2017, DeepQ has been committed to applying cutting-edge technologies, including artificial intelligence, generative models, and natural language processing, to address real-world clinical challenges and public health needs.

With a mission to build a secure, efficient, and human-centered smart healthcare ecosystem, DeepQ delivers solutions rooted in clinical priorities and patient well-being -whether it's accelerating AI model deployment in hospitals, implementing intelligent triage systems, or reducing administrative burdens for medical professionals.

To ensure the highest levels of information security and data protection, DeepQ has achieved internationally recognized certifications, such as ISO/IEC 27001, 27701, and ISO 27799, and has received multiple awards for innovation in medical technology and healthcare AI, underscoring its leadership and impact on the global stage.

Security remains the foundation of trust as healthcare moves toward a more intelligent and connected future. This whitepaper details how DeepQ integrates the principle of Security by Design from system architecture to cloud infrastructure to create a digital health environment that is secure, reliable, and trusted by both partners and end users.

DeepQ AI Platform

DeepQ AI Platform is an artificial intelligence solution developed by HTC's healthcare division specifically for medical imaging applications. It features a no-code interface that allows healthcare professionals without programming backgrounds to independently create, train, and deploy clinically relevant AI models.

Designed to support end-to-end medical AI workflows, the platform provides tools for medical image de-identification, annotation, model training, validation, deployment, and real-time inference. DeepQ also integrates directly with hospital Picture Archiving and Communication Systems (PACS), supporting seamless incorporation into existing clinical infrastructure and enabling efficient, AI-powered decision support.

To ensure hospitals and medical institutions can confidently adopt this platform, DeepQ is built with robust information security and privacy protection at its core. It adheres to internationally recognized standards and frameworks and is designed to meet the demanding requirements of clinical safety, data protection, and system reliability in regulated healthcare environments.

DeepQ AI Platform is an all-in-one artificial intelligence solution developed by HTC's healthcare division, purpose-built for medical imaging applications. With a no-code interface, the platform empowers healthcare professionals to effortlessly train and deploy clinically valuable AI models.

From de-identification and annotation of medical images to model training, deployment, and real-time inference, DeepQ AI Platform offers a complete and seamless AI development pipeline. It also supports direct integration with hospital PACS (Picture Archiving and Communication System), accelerating the digital transformation of clinical workflows.

Additional platform highlights include:

- Multi-model deployment with role-based authorization for flexible use cases
- AI Insight reports to evaluate and validate models prior to deployment
- Secure GCP-based cloud infrastructure with containerized microservices, disaster recovery, and end-to-end encryption

DeepQ AI Platform represents HTC's commitment to healthcare innovation, offering a trusted and scalable AI solution to advance medical intelligence with confidence.

Key Features of DeepQ AI Platform

- Data Management and Image Annotation
  - Medical imaging data is de-identified before processing to ensure patient privacy medical imaging data to protect patient privacy
  - Comprehensive annotation tools support classification, object detection, and segmentation
  - Strict control over annotation data quality and sourcing
- AI Model Training and Evaluation
  - Integrated optimization of AI models with automatic parameter tuning
  - A user-friendly no-code interface enables healthcare professionals to train AI models without programming expertise
  - AI Insight Reports offer transparent and detailed evaluation of model performance.
  - The platform proactively monitors training progress and **automatically halts training if the data quality or distribution is insufficient to produce reliable results**. It then provides actionable suggestions to improve the dataset before retraining, significantly reducing wasted time and computing costs.
- Real-time Model Deployment and Application
  - Supports real-time AI model deployment with rapid integration into medical imaging workflows (DICOM/PACS)
  - Multi-level user authorization settings to enhance deployment security
  - Complete inference history available for further analysis and model retraining

Security and Privacy Measures in DeepQ AI Platform

Deployment and Infrastructure

The platform offers flexible deployment models, including secure cloud-based and on-premises environments, to meet the varying data sensitivity and compliance requirements of healthcare institutions.

Cloud Security Controls

- Utilizing Google Cloud Platform (GCP) to deliver comprehensive security measures that ensure the protection of both data and services.
- Granular identity and access management (IAM) policies ensure only authorized users and services can access protected resources.
- Data at rest and in transit is protected using industry-standard encryption protocols.
- Network-layer security controls prevent unauthorized access and mitigate potential cyber threats.

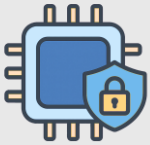
Pre-deployment Model Validation

All models undergo extensive validation and security testing, with detailed AI Insight Reports to assure accuracy and security

Identity Verification and Access Control

- Two-factor authentication (2FA) coupled with strict role-based access control (RBAC) mechanisms for secure access
- Role-based access control (RBAC) is strictly enforced to minimize the risk of unauthorized actions.

AI Model and Training Security



Protection of AI Models and Training Data

- AI models are stored securely in encrypted storage and training/inference are conducted within secure containers.
- Inference logs with personal health information are encrypted, password-protected, and subject to masking.
- Training Data is validated using Data Insight Reports to ensure quality and prevent data contamination.
- Pre-deployment model review is conducted by the internal deep learning team to ensure compliance and integrity.

Application and API Security

- Employs cloud-native protection mechanisms, including token-based authentication, policy-driven authorization, rate limiting, and web application firewall controls, to defend against DDoS attacks and common web application threats.
- Enforces granular permission control through role-based authorization frameworks to restrict unauthorized access.
- Conducts regular security scans and vulnerability assessments of user interfaces to detect and mitigate common web risks.

Monitoring and Event Management

- Implements real-time log monitoring and event notification mechanisms to ensure timely detection of anomalies and potential security incidents.
- Operation logs are retained in accordance with internal policies and regulatory requirements and are available for auditing and incident response purposes.

Disaster Recovery and Business Continuity

- The platform is designed with multi-region redundancy and resilient infrastructure to maintain service availability in the event of regional disruptions.
- Encrypted backup mechanisms and regular disaster recovery exercises are implemented to ensure continuity of operations and minimize the impact of unexpected incidents.

Account Management and Access Controls

Account access and administrative privileges adhere to the principle of data minimization. Administrative access is granted strictly on an as-needed basis, ensuring that individuals receive only the minimum level of access required for their responsibilities. All changes to access controls are documented and logged for review by authorized personnel.

DeepQ AI Platform empowers healthcare professionals to build reliable AI models with minimal effort, while intelligently reducing wasted computation by detecting poor-quality training data early and guiding users to correct it before continuing. With the DeepQ AI Platform, hospitals and medical institutions can securely and quickly deploy high-quality medical AI solutions, supporting the advancement of clinical services and accelerating the realization of smart healthcare.

DeepQ MedAgent

The DeepQ MedAgent is a generative AI-powered system that enables medical institutions to rapidly create, configure, and deploy intelligent assistants tailored to diverse clinical workflows.
Far beyond a traditional disease management tool, the platform empowers healthcare professionals to generate specialized AI agents through simple interactions—whether via conversation or click—streamlining communication, automating administrative tasks, and enhancing patient engagement.

With AI agents such as the Patient Education Agent, Scheduling Agent, and Documentation Agent, DeepQ MedAgent enables healthcare professionals to focus more on delivering high-quality care while reducing administrative burdens. This whitepaper provides detailed insights into the security and privacy measures implemented by DeepQ MedAgent, allowing healthcare institutions to confidently deploy and use the platform.

DeepQ MedAgent leverages modular AI agents to streamline both collaboration among care teams and direct communication with patients.
By automating routine interactions, delivering structured summaries, and supporting coordinated care across specialties, the platform reduces administrative workload and enables clinicians to focus on patient care. These agents operate at multiple points in the patient journey, enhancing workflow efficiency and improving communication across both internal teams and patient-facing interactions.

- Patient Education Agent: This agent handles common questions and delivers health education content automatically.
- Scheduling Agent: This agent understands voice or text instructions to set up, adjust, and manage communication schedules. It can trigger follow-up actions once the schedule is set.
- Documentation Agent: This agent generates requested documents based on consolidated clinical inputs.

Key Features of DeepQ MedAgent

- **Integrated Multi-Agent Platform**

  Supports multiple AI agents—including education, scheduling, and documentation—within a single system. Built-in safeguards and structured guidance help maintain response accuracy and clinical reliability.

- **Configurable Agent Activation**

  Agents can be enabled based on department, specialty, or stage of care. This flexibility ensures that support aligns with actual clinical workflows.

- **Human Oversight for Sensitive Content**

  For high-risk or sensitive communication, responses can be reviewed and approved before being sent. Institutions can define which scenarios require manual intervention.

The DeepQ MDM platform employs advanced cloud-based infrastructure with automated container management technologies to ensure stable, uninterrupted operations. Additionally, the platform includes robust cloud security mechanisms to effectively protect against cyber threats and ensure continuous service availability

Security and Privacy Measures in MedAgent

Model Security

AI models undergo rigorous testing and validation before deployment, ensuring stable and accurate operations. Any updates or retraining of deployed models follow strict version control and re-validation processes, with detailed logs available for audit purposes.

Access Control

DeepQ implements multi-factor authentication and role-based access controls, ensuring that only authorized personnel can access necessary medical information. Change in access control is logged for review by the authorized personnel.

Application Security

DeepQ places a strong emphasis on application and API security, providing secure authentication mechanisms and access controls. Measures are implemented to defend against common cyber threats, maintaining high service security standards.

Medical Image De-identification

Automatically de-identifies medical records and DICOM image data.

System Monitoring and Management

The platform includes comprehensive monitoring and management capabilities, enabling quick detection and resolution of anomalies, along with maintaining comprehensive, auditable operation records.

Disaster Recovery

DeepQ maintains geographic redundancy and regular data backups, coupled with periodic disaster recovery drills, ensuring continuity of healthcare services.

Data Ownership and Governance

All patient-related data remains fully owned by the healthcare institution. DeepQ adheres to strict data governance policies and does not use client data for training or analytics without explicit consent.

The DeepQ MedAgent provides healthcare institutions with a secure, adaptable, and clinically reliable foundation for deploying AI-driven assistants across a range of workflows. By combining modular agent design, human oversight, and enterprise-grade security, the platform supports efficient communication, reduced administrative load, and safer patient engagement in today's evolving healthcare landscape.

VIVE Arts

We believe technology is not merely about innovation, but also about expanding the boundaries of imagination. VIVE Arts exemplifies this philosophy, uniting cutting-edge technology with the timeless world of art, offering global audiences immersive cultural experiences that transcend the conventional.

VIVE Arts has collaborated with the world's foremost museums, cultural institutions, and contemporary artists. Through the application of Virtual Reality (VR), Extended Reality (XR), distributed ledger technology, and digital proof of ownership, we are redefining how art is created, experienced, and preserved.

Our vision is to harness technology to dissolve the barriers of time and space, connecting people intimately with creativity and cultural heritage wherever they are.

Art Without Boundaries

Pioneering new artistic frontiers

We empower artists with VR, XR, and emerging media, enabling them to craft works that transcend the senses, engaging sight, sound, and space alike.

Expanding audiences' horizons

Museums and galleries no longer have walls. From London to Tokyo, from Paris to New York, cultural treasures are now a heartbeat away, accessible from the comfort of your home or workplace.

Safeguarding cultural heritage for generations

Through digital preservation, we ensure that the masterpieces of human history endure, shared, celebrated, and reimagined for future generations.

Global Collaborations: Partnering with Icons

VIVE Arts has forged partnerships with more than 50 world-renowned cultural institutions, including:

- The Louvre: Bringing to life the genius of Leonardo da Vinci through immersive VR exhibitions.
- Tate Modern and Victoria and Albert Museum: Offering transformative encounters between technology and cultural narratives.
- The National Palace Museum (Taiwan): Fusing Eastern artistry with the latest immersive technologies to reawaken historical treasures.

Our collaborations extend to some of the most innovative voices in contemporary art:

- Albert Oehlen's *Basement Drawing*: A reimagining of the creative space, allowing audiences to step inside the artistic process.
- Wu Tsang's *of Whales*: A large-scale immersive installation showcased at the Venice Biennale, blending ecology and human storytelling.
- Hsin-Chien Huang and Laurie Anderson's *to the Moon*: A poetic lunar journey that melds artistic vision with digital innovation.

Exemplary Experiences

- **Versailles: The Lost Gardens of the Sun King**
  In collaboration with Château de Versailles, this VR experience transports viewers back to the opulence of 17th-century France, unveiling the grandeur of the Sun King's lost gardens.
- **Van Gogh's Palette**
  Step into Van Gogh's world and immerse yourself in his brushstrokes, emotions, and inspirations—within a virtual space where color and feeling seamlessly intertwine.
- **Le Bal de Paris**
  An extraordinary collaboration with choreographer Blanca Li, inviting audiences into a virtual ballroom where dance, music, and technology converge.

VIVE Arts remains steadfast in exploring emerging domains, including the Metaverse and art collections with digital certificates, as well as AI-driven creative expressions. Our mission is to empower the global art ecosystem's digital transformation, inviting broader participation and co-creation, and reshaping the very definition of art in the digital age.

VIVE Arts Platform

The VIVE Arts Platform is a pioneering global platform dedicated to showcasing and licensing diverse forms of digital art, including virtual reality (VR) and augmented reality (AR) content, as well as exclusive artworks with digital proof of ownership. It represents a vibrant convergence of creativity and cutting-edge technology.

VIVE Arts is an empowering community dedicated to fostering artistic innovation and creativity. It provides artists with essential technical support and resources, enabling them to leverage the latest XR and AI technologies.

Security and Privacy Measures in VIVE Arts Platform

Encryption Strategy

Data stored within the VIVE Arts Platform is encrypted by default using industry-standard encryption services. Encryption keys are securely managed through a centralized key management system, providing robust protection for data at rest and in transit. These practices align with global security standards and best practices

Data Backup and Restoration

Automated daily backups are maintained and retained in accordance with HTC's internal policies and data governance standards. A comprehensive disaster recovery (DR) framework is established, including regular drills and recovery validation tests to ensure service continuity during unexpected incidents. The system is designed to meet high availability (HA) and data integrity requirements.

Network Boundary Protection

Multiple layers of network defense are implemented, including firewall configurations and Intrusion Detection and Prevention Systems (IDS/IPS). Web Application Firewall (WAF) mechanisms are also in place to detect and block common attack vectors at the application layer. All configurations are periodically reviewed to maintain effectiveness.

Secure Communication Protocols

Communications across the platform are protected using advanced encryption protocols supporting multiple modern cryptographic algorithms. These protocols provide confidentiality, integrity, and authentication (CIA) across all data transmissions and are regularly reviewed.

Vulnerability Management

Regular source code scans, host vulnerability scans, and black-box testing ensure a comprehensive security assessment and proactive threat mitigation.

Cloud Infrastructure Security

The platform leverages Amazon’s secure cloud services (AWS), benefiting from their globally recognized security infrastructure and compliance. Strict Identity and Access Management (IAM) policies are enforced, alongside continuous monitoring for proactive threat detection and operational reliability.

Container Security

Containerized components undergo regular image scanning and are governed by granular access control policies. These measures ensure secure deployment and runtime isolation within the virtualized environment.

Log Management and Monitoring

Logging is implemented across the application, system, and network layers, capturing key events such as authentication attempts, data access, and system errors. Logs are securely synchronized and retained in accordance with defined policies.

Centralized Logging and Alerting

A centralized logging system is deployed to enable real-time monitoring and forensic analysis. Log data is encrypted in transit and at rest, with access strictly restricted based on roles (RBAC). Automated alert mechanisms flag unusual activities, such as privilege escalations.

Whether you're an artist, collector, or simply passionate about digital art, the VIVE Arts Platform offers the ideal space for exploring and engaging with the future of digital creativity. Join us and be part of the exciting intersection of art and technology.

Contact Us

For inquiries, please reach out to the appropriate contact list below:

- HTC Privacy: global-privacy@htc.com
- HTC Security: security@htc.com
- HTC VIVERSE: https://support.viverse.com/hc/en-us
- HTC VIVE (Enterprise Solutions): https://business.vive.com/enterprise_inquiry/
- HTC VIVE Mars CamTrack: https://www.mars.vive.com/contact-us
- G REIGNS: https://www.reignnet.com/contact
- VIVE ORIGINALS: https://viveoriginals.com/#ContactUs
- DeepQ: info@deepq.com
- VIVE ARTS: general@vivearts.com

This Security and Privacy Whitepaper is for informational purposes only and does not constitute any warranty (expressed or implied) or contractual commitment by HTC. Readers are encouraged to conduct their own research and seek guidance before making any decisions based on the information contained herein.