Trust & Security Center Overview

Tekle Holographics ("Tekle") prides itself on delivering cutting-edge holographic hardware and software solutions that enterprises can trust with their most sensitive data and critical operations. This Trust & Security Center Overview provides a comprehensive look at how we safeguard that trust. It details our approach to regulatory compliance, data security, system architecture, operational processes, and support practices that together form our security posture. Whether you are evaluating Tekle for deployment in a highly regulated industry or simply want assurance that we follow industry best practices, this document will answer those questions. We cover topics ranging from GDPR and ITAR compliance to encryption standards, from our secure development lifecycle to incident response readiness, and from deployment flexibility to the integrity of our partner ecosystem. Tekle is committed to transparency in these areas – we want you to know exactly what we do to protect your interests and how we continuously reinforce the trust you place in our solutions.

1. Data Protection & Privacy (GDPR Compliance)

Tekle Holographics is fully committed to data protection and user privacy. As a Netherlands-based company serving global clients, we adhere strictly to the EU General Data Protection Regulation (GDPR) and comparable data protection laws in all jurisdictions where we operate. In practice, this means we treat any personal data with the highest care and lawfulness. We collect only the minimal personal information necessary (often limited to business contact details, user login credentials, or telemetry required for system functionality), and we process it solely for the purposes agreed to by our customers. Tekle acts as a **Data Processor** on behalf of our clients (who are usually the Data Controllers for their end users' data). We have a robust Data Processing Addendum (DPA) that contractually binds us to GDPR's requirements – including commitments such as: processing personal data only on documented instructions from the controller, ensuring personnel handling data are under confidentiality obligations, implementing stringent security measures, assisting with data subject requests and breaches, and either returning or deleting personal data at contract termination. We also oblige any sub-processors (such as cloud hosting providers or support tools that might handle personal data) to sign similar DPAs, and we maintain a list of these sub-processors for transparency.

In terms of **data subject rights** and privacy practices: if an individual whose data is processed via Tekle's platform (e.g. an employee of our customer) requests to exercise GDPR rights like access, correction, or deletion, Tekle will promptly assist our customer in fulfilling those requests. We have established procedures to search, retrieve, and erase personal data upon verified request, and our systems are designed to facilitate such actions. Our **Privacy Notice** further details what data we collect and how we use it, and it is publicly available for all users of our services.

To bolster privacy, we apply the principles of **Privacy by Design and Default**. During product development, privacy implications are considered – for instance, features are built to use non-personally identifiable data where possible, and personal data fields are often optional or off by default unless needed for functionality. We also pseudonymize or anonymize analytics data; operational metrics we gather from devices are generally statistical or system-oriented rather than user-identifying, unless you explicitly opt in for certain personalized cloud services.

Cross-Border Data Transfers: For clients in the EU/EEA, Tekle can ensure that personal data remains within European data centers. If any data ever needs to be transferred outside of the EU (for example, if a customer's users collaborate with a device in another region, or for cloud service redundancy), we employ GDPR-approved transfer mechanisms, such as **EU Standard Contractual Clauses** with additional safeguards, to maintain compliance. We also monitor legal developments like the EU-US Data Privacy Framework to adapt our practices accordingly. At present, we do not engage in any voluntary sharing or selling of personal data to third parties for marketing or other external purposes – and we never will without explicit consent.

Privacy Governance: Tekle has an appointed Data Protection Officer (DPO) who oversees our privacy strategy and compliance. We conduct periodic data protection impact assessments (DPIAs) when introducing new features that involve personal data to ensure risks are identified and mitigated. All employees undergo privacy training, so they understand GDPR obligations and how to handle personal data. Through these measures, we create a culture of respect for privacy across the organization.

2. Export & Defense Compliance (ITAR and Beyond)

In addition to privacy regulations, Tekle Holographics complies with relevant export control laws and defense-related regulations, given that our solutions often serve military and aerospace projects. Notably, we align with the **International Traffic in Arms Regulations (ITAR)** and the U.S. Export Administration Regulations (EAR) when dealing with defense customers or any content that could be classified as controlled technical data.

Practically, ITAR compliance at Tekle involves several layers of control. First, we determine whether any aspect of our products or a customer's data is subject to ITAR's United States Munitions List (USML) or other export restrictions. Our holographic display hardware and standard software are generally commercial-off-the-shelf technology, but the **data** being visualized (e.g. classified schematics or mission plans) might fall under ITAR if it's defense-related. To accommodate this, Tekle offers deployment scenarios that keep ITAR-controlled data in secure environments accessible only by U.S. Persons. For example, if a U.S. defense client uses Tekle's system to visualize sensitive data, we can deploy our software on **U.S.-based servers or closed networks** that meet ITAR requirements, and ensure that support is handled by U.S. Person staff when necessary. We have partnerships or subcontractor arrangements in the United States to provide local support under ITAR-compliant conditions (including technical assistance agreements if required). All Tekle personnel who may come into contact with ITAR data (even incidentally, such as during troubleshooting) receive training on ITAR regulations and must be explicitly authorized. We maintain export control policies internally that cover classification of technology, obtaining export licenses when needed, and screening of transactions and end-users against prohibited parties lists.

Beyond ITAR, Tekle also respects other defense and dual-use regulations. For instance, as a Dutch company, we comply with the EU and Dutch export control rules (including the Wassenaar Arrangement for dual-use technologies) – ensuring we don't export controlled technology or technical information to embargoed countries or entities. If our holographic devices are shipped internationally, we work with the relevant authorities to get any necessary export license. We also label and document hardware properly for customs to prevent unauthorized diversion.

By weaving compliance into our operations, Tekle can confidently serve highly regulated sectors. Clients in defense, aerospace, or other government domains can rely on us to handle classified or controlled data properly. We also are open to signing specialized agreements (like ITAR Technology Control Plans) and undergoing security inspections if that's part of a project's requirements. Our goal is to be a trusted partner that **meets or exceeds** the legal standards for security in every jurisdiction we operate.

3. Cloud Hosting, Encryption & Data Security Controls

Tekle's technical infrastructure is built on secure, high-performance cloud hosting combined with strong encryption and access controls, providing a rock-solid foundation for our applications. We host our cloud services on **leading providers such as Microsoft Azure** (and also utilize Amazon Web Services in certain cases for redundancy and client-specific needs). These providers offer state-of-the-art physical security, network protections, and a broad compliance portfolio (certifications like ISO 27001, SOC 2, FedRAMP, etc.) that we inherit for the portions of our service running there. All servers are kept up to date with security patches and hardened according to industry benchmarks (for example, we apply CIS hardening guidelines to our virtual machines and container environments). We isolate environments by client and by purpose: development, testing, and production systems are separated to reduce risk, and each customer's data is logically segregated (with unique identifiers and access tokens) in our multi-tenant cloud database.

Encryption: We implement encryption rigorously. All data at rest in our databases, file storage, and backups is encrypted using strong algorithms (generally AES-256). This means that even if storage media were compromised, the data would be unreadable without the proper keys. Those encryption keys are managed using secure key management services provided by our cloud platforms, and keys are rotated periodically. In transit, all communications – whether between a user's client application (or device) and our cloud, or between our devices and any server – are protected by TLS encryption. We force HTTPS/TLS 1.2+ for all API calls, web portals, and data transfer streams, ensuring no data travels over the network in plaintext. We also support modern cipher suites and enable features like Perfect Forward Secrecy for enhanced security. For on-premises deployments (where the system might run entirely on a local network), we still use encryption for data flows between components, so internal network traffic is protected especially in scenarios where an insider threat is a concern.

Access Controls: Tekle uses robust access control mechanisms at multiple levels. At the application level, our platform has a role-based access control (RBAC) system allowing administrators in your organization to define roles (e.g. Viewer, Designer, Administrator) and set permissions for who can view holographic content, make changes to models, manage system settings, etc. This ensures users only access the functions and data appropriate to their job. We also offer integration with corporate identity systems – for example, our cloud services can integrate with SAML 2.0 or OAuth2 for Single Sign-On, so that you can use your enterprise Identity Provider (like Azure AD or Okta) to authenticate and provision Tekle users. This not only simplifies user management but leverages your existing multi-factor authentication (MFA) and password policies for added security. Tekle strongly encourages enabling MFA for any

administrative or privileged access to the system, and we support TOTP-based or IdP-based MFA as part of our SSO integration.

On the infrastructure side, access control is equally strict. Administrative access to Tekle's cloud servers or databases is limited to a handful of operations engineers and is only possible through secure channels (VPN with hardware token MFA + individual SSH keys, for example). All such access is logged and monitored. We employ the principle of **least privilege** – our team members only have the minimum access necessary to perform their role, and temporary access (just-in-time provisioning) is used for sensitive operations so that even authorized personnel don't retain continuous high-level access. Within our development environment, we segregate duties: developers cannot directly access production data, and support engineers may get access only when needed to resolve a customer issue and only to the extent necessary (often using anonymized or test data where possible).

Monitoring and Protection: Our cloud infrastructure is instrumented with security monitoring tools. We use Intrusion Detection/Prevention Systems (IDS/IPS) and continuous vulnerability scanning on our network perimeter. We also deploy endpoint protection on our servers to detect malware or abnormal behavior. Automated alerts will notify our security team of potential issues like multiple failed login attempts, unusual data download patterns, or changes to critical system configurations. DDoS protection services from our cloud providers are enabled to mitigate denial-of-service attacks, keeping services available. In addition, database-level encryption and row-level security ensure that even within the database, each client's data can only be queried by that client's context.

Data Residency & Localization: We recognize that data sovereignty is vital for many clients. Tekle's cloud can be deployed to specific regional data centers based on customer preference – e.g. Europe (for EU data residency), North America, or Asia-Pacific regions. When we set up a customer's cloud environment, we do so in the region closest to their operations or in a region they mandate. All data (including backups and replicas) then stays within that geographic jurisdiction. For government clients, we also have the capability to work with sovereign cloud offerings (such as Azure Government for US public sector, which is managed by screened U.S. personnel) if required.

Secure Configuration: Out of the box, our devices and software come configured with secure defaults. Default passwords or credentials are never hard-coded; each device in the field has a unique bootstrap credential that the customer is prompted to change upon installation. Services on the device that are not needed are disabled or firewall-restricted. We frequently review our configurations against emerging threats – for example, ensuring that no older, vulnerable protocols (like SMBv1 or older SSL versions) are enabled.

Tekle's approach to hosting and data security is to blend the best security features of modern cloud infrastructure with careful control by our team and our customers. **Your data's security and sovereignty are paramount**, and our combination of encryption, access control, and monitoring provides a strong defense in depth to protect it.

4. Secure Development & Lifecycle Management

Security is not a one-time effort at Tekle; it's an ongoing process woven into our product lifecycle. This section details how we build and maintain our software and systems securely over time.

Secure Development Lifecycle (SDL): We have adopted a Secure Development Lifecycle framework that guides our engineering teams. Key aspects of Tekle's SDL include:

- **Secure Design:** In the planning phase of a new feature or product, our architects incorporate security requirements alongside functional requirements. We perform **threat modeling** to anticipate how a feature could be misused or attacked, and we design appropriate safeguards. For example, when designing a cloud syncing feature, we consider threats like man-in-the-middle attacks or unauthorized access, and then specify encryption and authentication steps to counter them before coding begins.

- **Coding Standards:** Our developers follow coding standards that emphasize security (for instance, validating inputs to prevent injection attacks, careful memory management in C++ modules to avoid buffer overruns, etc.). We prefer using safe libraries and frameworks that have built-in security features – such as leveraging proven cryptographic libraries instead of writing our own. Peer code reviews are mandatory for any significant code change, and part of that review checklist is "check for security impacts". We also maintain an internal secure coding guide that is updated regularly with lessons learned from past vulnerabilities or industry incidents.

- **Automated Scanning & Testing:** During implementation, we use **static application security testing (SAST)** tools that scan our source code for known vulnerability patterns (like use of deprecated cryptographic functions, potential SQL injection, cross-site scripting in any web components, etc.). Our build pipelines include these scans, and any high-severity findings break the build so they must be addressed. We also employ **dependency scanning** to track third-party libraries for known vulnerabilities (via databases like CVE/NVD). If a critical vulnerability is announced in a library we use, our policy is to patch or upgrade that dependency within a defined timeframe (often 1-2 weeks or faster if actively exploited). In addition to static testing, we use **dynamic application security testing (DAST)** on running applications – for example, simulating web attacks on our management portal or API fuzzing to see if any unexpected input causes a security failure.

- **Penetration Testing:** Tekle engages independent security firms periodically to perform **penetration tests** and ethical hacking exercises on our products. At least annually – and more often for major releases – these third-party experts test our cloud services, device firmware, and client applications for vulnerabilities. We receive detailed reports of any findings and prioritize fixing them immediately. We also run internal "red team" exercises where our internal security engineers act as adversaries to test our detection and response (these exercises help improve both the product and our operational security).

- **Hardening & Deployment:** Before deploying new systems or updates, we ensure that configurations are hardened. Default admin accounts are removed/disabled, secure configurations are applied as mentioned earlier, and any debug interfaces or test code is stripped out of production builds. We maintain separate environments for testing and staging, where security tests are repeated before final rollout. Infrastructure-as-code is utilized to replicate secure settings reliably across deployments.

- **Continuous Improvement & Maintenance:** After release, we remain vigilant. Tekle monitors news of vulnerabilities in any components we use (operating systems, libraries, etc.) and patches our products accordingly. We release security updates proactively – in some cases, we've pushed emergency patches within 24-48 hours of a critical vulnerability disclosure affecting our stack. Our continuous delivery approach (with updates every few weeks) enables us to deliver improvements and fixes rapidly . For customers with on-prem installations, we provide these updates in a timely manner and work with their change management processes to apply patches as soon as possible. We also welcome and facilitate security upgrades; for example, if a better encryption standard becomes available, we plan and implement the transition (such as moving from RSA to elliptic-curve algorithms, or from SHA-256 to SHA-3, as standards evolve).

- **Security Training and Awareness:** We recognize that tools and processes are only as effective as the people using them. Tekle runs mandatory security training for all engineers annually, with additional targeted training for those working on critical security-sensitive code (like authentication modules or encryption features). We cover topics like secure coding, recent incident case studies, social engineering awareness, etc. Developers also participate in capture-the-flag style security challenges internally to sharpen their skills and keep security thinking fresh. This culture of security awareness helps prevent mistakes and encourages team members to flag potential issues early (often even before code is written, an engineer might raise "is this design secure?" in planning meetings – an attitude we strongly encourage).

- **Secure Configuration & Secrets Management:** Within our development and operations, we manage sensitive data (like credentials, API keys, certificates) using secure vaults. No passwords or secrets are hard-coded; they are injected at runtime from encrypted vault stores and rotated regularly. We also avoid embedding any secrets in our distributed software – for instance, the firmware on a Holo-Table has no universal password or backdoor, and any factory credentials are randomized per device and provided securely to the client.

Lifecycle Governance: Tekle's management regularly reviews our security roadmap and practices. We perform annual internal audits on our SDL process to ensure it's followed (for example, verifying that threat models and code review checklists are documented for key projects). These audits may be used in compliance efforts or certification processes in the future (as we aim to align with standards like ISO 27001 in our information security management).

Tekle's development lifecycle doesn't treat security as a checkbox – it's an integral quality metric for our products. By the time you install a Tekle solution, it has been through rigorous security design, testing, and validation steps. And our work doesn't stop at delivery; we continually improve and support the product to adapt to the evolving cyber threat landscape.

5. Deployment Models & Architecture

Tekle's solutions are versatile in deployment: whether you choose our managed cloud service, an entirely offline on-premise setup, or something in between, the architecture is designed for security and performance. Here we outline each model and the architectural considerations.

- **Tekle Cloud (Managed SaaS):** In the cloud model, Tekle hosts the server components of the solution in our cloud environment. This includes the data storage (for model files, user data, logs), coordination servers for multi-user collaboration, and any web portals or APIs for managing content. The customer accesses the system via lightweight client applications (e.g., the holographic device's client software and a web dashboard) over the internet. The **architecture** here is multi-tier: the client app authenticates to a cloud API gateway, which communicates with backend services (for model rendering, user management, etc.) and databases. We use load balancers and auto-scaling to ensure reliable performance as usage grows. Each customer tenant is isolated at the application layer – they have separate data stores and access contexts, enforced by our software logic and cloud security groups. For additional security or compliance, we can also provision dedicated instances or VPCs (Virtual Private Clouds) for a single tenant, which some enterprise customers opt for to have an extra layer of isolation (a single-tenant cloud deployment). The advantage of Tekle Cloud is that we handle all the infrastructure management, patching, and scaling, and customers always have the latest features without needing to upgrade hardware. We also implement **multi-region redundancy** for critical cloud services – for example, data is backed up in a secondary region and our services can failover if an entire region goes down, which contributes to our disaster recovery capability. From a network perspective, customers connect to Tekle Cloud over secure HTTPS; no inbound connections to customer networks are needed, simplifying firewall configurations.

- **On-Premises / Offline Deployment:** In this model, the customer runs the entire Tekle solution within their own environment with *no* dependency on external networks. Typically, a Tekle on-prem deployment might consist of one or more **holographic display devices** (e.g., Holo-Table or Holo-Wall units) and a local server or workstation that acts as the data/content server for those devices. The architecture is essentially a miniaturized version of the cloud on your premises: the server hosts the collaboration and storage functions, and the devices and any user PCs connect to that server over a local area network (LAN). We provide the necessary server software for installation on a Windows or Linux server (or we can provide a pre-configured appliance if desired). All communication stays within the LAN, and we work with your IT team to ensure the system meets your network segmentation requirements (for instance, it can be placed on a dedicated VLAN or closed network). Because this deployment is offline, certain cloud-specific features (like remote multi-site collaboration or cloud backups) would be disabled or replaced with local equivalents. We ensure that the software can function fully in a stand-alone mode – license checks or user authentication can be done locally

(with license files and offline user management tools provided). One key architectural consideration is updates: for offline systems, Tekle supplies update packages that an administrator can apply manually; no automatic cloud update will occur. Security-wise, an on-prem deployment can be as secure as the environment it's in – since data never leaves your facility, it's protected by your perimeter. We supplement that by hardening the provided software/appliance and by not requiring open ports to the internet. Many defense clients choose this option to comply with air-gapped network policies. We have successfully deployed fully offline systems that operate in classified lab environments, for example.

- **Hybrid / Self-Hosted Cloud:** Some clients prefer to host Tekle's server components in their own private cloud or data center (perhaps to leverage existing enterprise cloud infrastructure or to satisfy internal policy, while still maintaining some remote access capabilities). In this scenario, Tekle provides a **self-hosted server software package** (which can be delivered as containers, virtual machine images, or installation scripts) that the client's IT team deploys on their chosen environment (could be on their Azure/AWS tenant, or on physical servers in a data center). The architecture then is under the client's control but follows our reference design: typically a database, an application server, and optionally a web front-end component. We assist with initial configuration to ensure security settings mirror our standards. Once deployed, end-users can access the system much like the Tekle-managed cloud (over the internet or corporate network), but all data and processing reside in the client's cloud environment. This model provides a middle ground wherein you get the **control and data residency** of on-prem, but the convenience of enabling remote access for your users through your own cloud setup. For example, a large enterprise might deploy Tekle's server in their Azure subscription in a region of their choice; their global offices then connect to that, and since it's under their Azure, they can integrate it with their central logging, identity management, and monitoring systems. Tekle's hybrid architecture supports such integration – e.g., connecting to your corporate monitoring (we can output logs to your SIEM system), using your identity provider tokens for auth, etc. We also allow hybrid scenarios like **occasionally connected** modes: say most of the time your system is offline, but you can periodically connect it to the internet to fetch updates or allow a short collaborative session with another site, then disconnect – Tekle's software can sync data when connected and operate standalone when not.

Across all these models, the core holographic rendering engine and user experience remain consistent. The difference lies in where the "brains" (server logic and storage) reside and who manages them. Importantly, we ensure **security equivalence** among the options: the same encryption standards, authentication protocols, and fine-grained access controls are in effect, whether it's Tekle cloud or your own data center. We do not for example use any less secure authentication for local deployments – it's the same robust mechanism, just without the internet. Likewise, our device hardware (the holographic displays) are identical in capability and security features regardless of deployment; in cloud mode they talk to cloud endpoints, in on-prem mode they talk to your local server – but in both cases, communications are encrypted and authenticated.

Network Architecture Considerations: For IT departments, integrating Tekle solutions is straightforward. In cloud deployments, only outbound HTTPS connections to Tekle's domains are required from the devices/users; many clients simply allow those through their firewall. In on-prem deployments, the system can be entirely closed off; if remote support is needed, options like temporary VPN or support tunnels at your initiation can be used, but by default nothing calls out. We can operate under strict firewall rules and even without DNS (offline modes can use static IP configuration). For hybrid, it's under your control, so it will follow your network design (we often provide a reference architecture showing required ports between components, etc., to assist your planning).

Tekle's deployment flexibility ensures that our solution can fit into high-security environments and existing IT ecosystems. We have invested in making each mode secure and feature-rich, so you can choose the option that balances your needs for control vs. convenience. Our team is also available to help with **architecture planning** – we often work closely with client IT and security architects to validate the design against their security requirements (be it penetration zone placement, compliance checklists, or performance testing in their network). The result is a tailored deployment of Tekle's technology that you can trust wholeheartedly, because it's configured on your terms without sacrificing the benefits of our platform.

6. Integration & Extensibility (RealityBridge and THSDK)

One of Tekle Holographics' core strengths is its ability to integrate with your existing enterprise tools and data. We know that our holographic displays will be one part of a broader ecosystem, so we've developed both out-of-the-box integration capabilities and customizable SDKs to ensure a smooth workflow. This section details how you can bring data into Tekle's platform and extend our functionality safely.

RealityBridge – Connecting to Your Data: RealityBridge is our suite of built-in connectors and plugins for third-party software. Out of the box, Tekle supports integration with major **Building Information Modeling (BIM)** and design applications. For instance, we provide a plugin for Autodesk Revit that allows a user to export or live-sync a BIM model to a Tekle holographic display with just a few clicks. Similarly, we have integration for Autodesk Navisworks to bring in aggregated models. These plugins maintain the metadata and structure of your models, meaning that what you see in holographic form is a faithful, interactive representation of your original design – complete with attributes, layers, etc. Additionally, RealityBridge supports **geospatial data integration**: you can link GIS datasets (such as ESRI shapefiles or services) to visualize real-world terrain, city models, or infrastructure data holographically. We partner closely with GIS platforms; for example, Tekle can consume data from ArcGIS Online or ArcGIS Enterprise through secure API access (using your credentials) to pull in map layers and then render them in 3D. Another integration aspect is point-cloud data: as noted in our product materials, Tekle software can ingest point cloud files (e.g. e57, las, laz) often produced by lidar scanners. This is incredibly useful for construction or digital twin applications – you can compare a scanned "as-built" point cloud to the "as-designed" BIM model within the hologram to spot discrepancies.

From a **security standpoint**, these integrations are handled carefully. Any plugin that interacts with external software uses authenticated channels and respects the security model of that software. For example, our Revit plugin will require the user to have appropriate Revit access – it simply acts as a bridge to push the model to Tekle, but doesn't circumvent any file permissions set in Revit or your BIM management system. If data is transferred to Tekle's cloud as part of integration (in cloud deployments), that transfer is encrypted and occurs via an API endpoint that requires an API key or user auth. In local deployments, the transfer might be direct over LAN – still encrypted. We ensure that intermediate files (like an exported model) are not left unprotected on disk; any caching we do is in encrypted form or within secure memory.

Tekle Holographics SDK (THSDK): For more advanced integration or custom application development, THSDK is our answer. The Tekle Holographics SDK provides programmatic access to the capabilities of our holographic displays. With THSDK, developers can write software that, for example, opens a holographic viewport in a custom simulation software, or that controls hologram content based on external events (like IoT sensor readings or a training simulation script). We supply THSDK plugins for **Unity** and **Unreal Engine**, two of the most popular 3D engines . This means if you have developers versed in those engines, they can quickly get started – they can create a Unity scene, import our SDK package, and then drive a Tekle display as an output device for that scene. This opens up enormous possibilities: our clients have used it to build custom training simulations where multiple holographic figures are animated based on AI inputs, or to integrate a Tekle Holo-Wall into a command center application showing real-time network cyber threats in 3D. The SDK also provides APIs for non-graphics integration: for instance, you can programmatically load models, adjust hologram parameters, or retrieve user interaction events (like where a user touched or pointed on the hologram) to feed them back into your system.

Maintaining Security in Custom Integrations: While the SDK gives a lot of power, we also provide guidelines so that custom integrations remain secure. Documentation includes best practices on handling authentication (for example, if your custom app connects to Tekle cloud, it should use OAuth tokens we issue rather than embedding credentials). We also isolate the SDK runtime environment – if a custom Unity app is run on a Tekle device, it runs in a sandboxed process with limited permissions, so a bug in a custom app can't easily affect the device's core system or other clients. Moreover, any network communication done through our libraries still goes through our encrypted channels. If a developer writes something truly from scratch using our lower-level APIs, we encourage using our provided client libraries which enforce encryption and error-checking, rather than trying to write raw packets. This ensures the consistency of security implementation.

Interoperability and Standards: Tekle is actively involved in the **Metaverse Standards Forum** and other initiatives to promote interoperability in 3D content and XR systems. Our goal is to support emerging standards like glTF for model formats, OpenXR for device interfaces, and real-time streaming standards for volumetric data. As these standards mature, we will incorporate them, allowing Tekle's ecosystem to connect even more broadly in a standardized way. This means in the future you could use third-party tools to create content in a standard format and load it into Tekle displays seamlessly, or vice versa, without custom adapters – all while preserving secure handling of the data.

In short, Tekle's integration ecosystem is both **rich and secure**. Whether you use our plug-and-play connectors to common software or dive into custom development with THSDK, we ensure that your data flows and integrations operate within a safe framework. Enterprises often find that Tekle slots into their existing pipeline with surprising ease – architects continue using their CAD and BIM tools, and Tekle just becomes another export target (but one that brings their designs to life in 3D). Developers find that they can build on Tekle for specialized needs without worrying about compromising the underlying system's security or stability. By prioritizing secure integration capabilities, Tekle extends its value across your enterprise while safeguarding the integrity of all systems involved.

7. Supply Chain & Partner Security

Delivering a secure product isn't just about the product itself – it's also about the security of every link in the chain that produces and supports that product. Tekle Holographics takes supply chain security seriously and works only with trusted, vetted partners in all aspects of our business.

Hardware Supply Chain: Our holographic devices (such as Holo-Table PRIME, Holo-Wall PRIME, etc.) are composed of high-quality components sourced from established manufacturers. We maintain close relationships with these manufacturers – many of which are based in Europe, Japan, or the US with strong quality control standards. Before selecting a supplier, our hardware team evaluates their security practices (for example, verifying that firmware provided in components like tracking cameras or projectors has no known vulnerabilities or hidden backdoors). We require certificates of origin and authenticity for critical components to guard against counterfeit parts. When components arrive at our assembly facility, they undergo inspection and testing. We flash our own secure firmware onto devices where applicable, using cryptographic signing to ensure that only Tekle-approved firmware runs on the hardware. Our devices have secure boot enabled, meaning they will not run unapproved low-level code – this protects against tampering in transit or at customer sites. For any device that stores data (like the computing unit inside a Holo-Table), we encrypt any sensitive data on it and provide mechanisms for customers to wipe or destroy data if a device is decommissioned. By controlling the hardware supply chain tightly, we minimize the risk of physical or firmware compromise.

Software Supply Chain: Modern software often relies on open-source or third-party components. Tekle manages this by maintaining an up-to-date inventory of all open-source libraries and third-party SDKs we use. Each of these is reviewed for security (we check things like whether the project is active, has had any major security flaws, and how those were handled). Where feasible, we use libraries that are widely trusted and even consider static linking or vendorizing code to avoid runtime dependencies that could be manipulated.

We also monitor the supply chain through tools that alert us if any of our source code dependencies are later compromised (for example, if an upstream maintainer account is hijacked and inserts malicious code, which unfortunately has precedent in the industry). Our build system uses cryptographic hashes to pin dependencies, so we don't inadvertently pull in a malicious update. Additionally, our software releases (installers, executables, updates) are digitally signed by Tekle. This allows customers to verify that the software they install is authentic and unaltered since it left Tekle's build environment.

Logistics and Delivery: When we ship physical products, we do so securely. Devices are sealed with tamper-evident seals. For especially sensitive deliveries (like to defense facilities), we arrange secure transport options and provide chain-of-custody documentation. If a device arrives and a tamper seal is broken, we advise clients to quarantine it and notify us for investigation. We can also perform on-site verification of device integrity if required.

Partner Vetting: Tekle often works with integration partners or resellers who help deliver and support our solutions in various regions or industries. We have a thorough vetting and certification program for these partners. It includes background checks on the company's history, checking references from other tech vendors, and ensuring they have qualified personnel. We train our partners in installation and support procedures, emphasizing security configuration. Partners must agree to our code of conduct, which includes protecting customer data, respecting IP, and reporting any incidents or vulnerabilities they observe. We limit the access partners have – for instance, a reseller might assist a customer on-site, but they won't have backdoor access to Tekle's cloud or customer data unless explicitly granted by the customer for support reasons. Essentially, they operate under the customer's supervision, or under Tekle's supervision if subcontracted, rather than autonomously having system access.

Service Providers: Tekle also utilizes third-party services for certain business functions (for example, a CRM system for sales, a cloud service for customer support ticketing, etc.). For any service that could involve personal data or confidential information, we ensure a **Data Protection Agreement** is in place (mirroring GDPR requirements) and that the service provider has adequate security certifications (such as ISO 27001 or SOC 2). We perform risk assessments for these providers as part of our vendor management program. If a provider doesn't meet our standards, we either don't entrust them with sensitive data or we implement compensating controls (like additional encryption or anonymization before data goes to them).

Internal Security & HR: Our own staff are a key part of the supply chain. Every Tekle employee and contractor goes through a screening process at hiring – this can include reference checks, identity verification, and in some cases criminal background checks (aligned with local employment laws). Staff in sensitive roles (like those who administer cloud systems or have access to customer data for support) are required to have higher-level vetting and must participate in regular security training. We enforce separation of duties; for example, the person who prepares a software release is not the sole approver for pushing it to production – another person reviews and approves it, preventing a single rogue employee from injecting something malicious. We also use the principle of four-eyes in critical operations (at least two authorized people must be involved to execute certain tasks, such as accessing encryption key material or initiating a data wipe).

If an employee leaves the company or changes roles, our off-boarding process promptly revokes their access to systems and any company devices are secured. This prevents former employees from retaining any unauthorized access.

Continuous Monitoring of Supply Chain: Tekle stays informed about broader supply chain security issues in the industry. For instance, if there's news of counterfeit chips affecting certain hardware or a breach at a supplier company, we reevaluate our exposure and take action (perhaps pausing use of a component batch, or applying patches if a partner software was compromised). We also maintain cybersecurity insurance that covers supply chain incidents, and we have an incident response extension that deals with scenarios like a tainted update or a supplier breach (so we treat it with the same urgency as a direct breach).

Tekle's holistic approach to supply chain and partner security ensures that our customers receive a product that is secure not only in design and implementation, but also in origin. When you deploy Tekle's solutions, you can be confident that **every link** – from the chips on the circuit boards to the technicians installing the system – has been considered through the lens of security and trustworthiness.

8. Incident Response, Business Continuity & Audit Trails

Despite best efforts in prevention, incidents can happen. Tekle has established robust processes to respond to security incidents or outages swiftly and transparently, minimizing impact and learning from every event. In parallel, we maintain business continuity plans to keep our services running through adverse conditions, and we ensure detailed audit trails are available for accountability and compliance.

Incident Response Plan: Tekle's Incident Response Plan (IRP) outlines specific steps for various types of incidents (security breach, malware outbreak, service outage, etc.). The plan is modeled on the NIST Incident Handling guide and is regularly updated. Key elements include:

- **Preparation:** Our team is trained on the IRP and each member knows their role. We have designated an Incident Response Team (IRT) that includes security engineers, system administrators, communications leads, and relevant product owners. We maintain an on-call rotation so that expert responders are available 24/7 in case of an emergency. We also have contacts at our cloud providers to reach out to if an incident is related to underlying infrastructure (for example, Azure's security team).

- **Detection & Analysis:** We deploy multiple layers of monitoring to detect incidents. Security alerts from our IDS/IPS, suspicious log events (e.g., an admin login from an unusual location), or automated service health alarms (like a spike in error rates) all feed into our centralized alerting system. We also provide channels for customers or researchers to report issues (which ties into our Vulnerability Disclosure program). Once an alert is received, our IRT follows a predefined analysis process: gather indicators, determine the nature and scope of the incident, and classify its severity. We have internal playbooks for common scenarios – e.g., "Credentials Compromised" or "DDoS attack" – which list specific analysis and containment steps.

- **Containment:** Upon confirming a security incident, our immediate goal is to contain the damage. Depending on the case, this could mean disconnecting a compromised server from the network, revoking certain user tokens, pushing a configuration update to block an IP address, or even temporarily taking a service offline to prevent further harm. We balance containment with operational continuity – for example, if one customer's account is affected by a breach (say their admin credential was leaked), we can isolate that tenant in the cloud environment without shutting down service for others. Our architecture's tenant isolation aids in containment as well.

- **Eradication:** After containing the threat, we work to eliminate the root cause. This could involve removing malware, applying a security patch, resetting passwords, or restoring clean backups. If the incident is a data breach, eradication includes making sure any unauthorized access is cut off and plugging whatever vulnerability was used. We also conduct forensic analysis in parallel to understand exactly what happened – we might capture memory images or log files for deeper investigation, often with the help of forensic experts if it's a serious breach.

- **Recovery:** We restore systems to normal operation once it's safe. Recovery steps might include bringing servers back online, monitoring them extra closely for any sign of recurring issues, and verifying integrity (ensuring that no backdoors or lingering malware remain). In cases of outages, recovery might mean switching to a backup system or scaling infrastructure to handle after-effects (like backlogs of data to process). We test affected systems thoroughly post-incident to confirm they're secure and stable.

- **Notification & Communication:** Transparency with our clients is critical during incidents. If an incident involves customer data or a significant service disruption, Tekle will notify affected customers promptly, providing as much detail as we can at the time. Our communications team has templated incident notifications ready, which include the nature of the incident, what data or services are impacted, what we're doing about it, and any steps we recommend the customer take (such as resetting their passwords, or in rare cases, temporarily disconnecting a device). For broader incidents (for instance, a widespread vulnerability like "Log4Shell" that required emergency patches), we also publish security advisories on our website and customer portal, keeping all customers informed even if they were not directly affected, so they know Tekle is addressing such industry-wide issues. We comply with any regulatory notification requirements as well – for example, if personal data is breached, we follow GDPR's mandate to notify supervisory authorities and data controllers within 72 hours, providing the necessary information.

- **Post-Incident Review:** After resolving an incident, Tekle conducts a post-mortem analysis. The IRT and relevant stakeholders meet to document the timeline, identify what went well and what could be improved, and enumerate **lessons learned**. Importantly, we then take action on those lessons – this could result in updates to our processes (maybe our monitoring missed a signal, so we add a new alert), additional training for staff, or enhancements to the product's security features. Every incident, whether minor or major, is viewed as an opportunity to strengthen our defenses and response.

Business Continuity & Disaster Recovery (BC/DR): Apart from targeted security incidents, Tekle plans for continuity in the face of natural disasters, infrastructure failures, or other large-scale crises. Our Business Continuity Plan outlines how critical operations will continue under various scenarios (e.g., primary data center outage, pandemic affecting our workforce, etc.). We utilize geographically distributed infrastructure – for our cloud services, data is regularly backed up to a secondary geographic region. We have defined **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO)** for our services; for instance, we aim for an RTO of a few hours for major cloud service interruptions (maximum downtime), and an RPO of close to real-time for user data (minimal data loss by using frequent replication). To achieve this, key systems have failover nodes and our databases use point-in-time recovery backups. If an entire region goes offline, our failover plan is to switch to the secondary region after verifying integrity, and DNS entries are updated to redirect users – this procedure is tested in drills.

For on-premise deployments, continuity relies more on the client's IT environment, but Tekle supports by providing backup mechanisms (e.g., the local server can be set up in a high-availability pair, and we offer tools to backup the hologram project data periodically to an offline medium). We document recommended DR procedures for clients who run self-hosted Tekle servers, including how to re-install a fresh server and restore data from backup in case of a corruption.

Internally, we maintain redundancies for our development and support operations as well. All critical internal systems (like code repositories, support databases) have cloud backups and can be operated remotely if our office is inaccessible. The COVID-19 pandemic was a real-world test of our business continuity, during which Tekle's teams successfully transitioned to remote work without interruption to our development or customer support.

Audit Trails and Logging: Across our products and services, Tekle generates detailed logs that serve as audit trails for actions. In the **Tekle Cloud**, every user login, data upload/download, and administrative action is logged with timestamp, user ID, and source IP. Similarly, on devices, actions such as starting a session, changing a setting, or pairing with another device are recorded in local logs. These logs are crucial for forensic analysis (as mentioned, we use them if investigating an incident) and also for customer compliance needs. Many customers in regulated industries need to maintain audit trails of system use – Tekle facilitates this by making logs exportable or accessible in a secure manner. For instance, a customer admin can request an audit report of all user activities in the past month via our admin portal, or they can choose to integrate Tekle logs with their centralized Security Information and Event Management (SIEM) system. We support log formats like JSON or syslog forwarding to make integration with tools like Splunk or Azure Sentinel easier. The logs are protected from tampering: in cloud, they are stored in write-once mediums with integrity checks; on devices, logs are appended in a way that users cannot alter past entries without detection (if higher assurance is needed, we suggest procedures like copying logs to an immutable storage or enabling system features akin to Windows Event Log's security log which requires admin privileges to clear).

Regular Audits and Assessments: In addition to logging user actions, Tekle periodically performs audits of its own security controls. We arrange for annual penetration tests (as noted) and also compliance audits when necessary for clients (for example, a client might request an audit or certification; we can work with them or an independent auditor to let them assess our controls). We are working towards formal security certifications in the future as our enterprise client base grows, and our current practices are aligned to meet those standards.

Overall, Tekle's incident and continuity program is about being **ready for the unexpected** and ensuring that our customers' operations are resilient. From immediate incident handling to long-term data retention, we strive to leave no stone unturned in planning for reliability. And through comprehensive audit trails, we provide both ourselves and our clients the means to verify and trust that the system is being used and managed appropriately.

9. Enterprise Support & Procurement Commitments

A crucial component of trust is knowing that your vendor will be there to support you and stand behind their promises. Tekle Holographics has established clear agreements and support structures to make our enterprise engagements smooth and reliable. This final section covers our standard agreements (MSA, DPA, SLA) and the support services we provide to back them up.

Master Service Agreement (MSA): Tekle's Master Service Agreement is the cornerstone contract that governs our relationship with enterprise customers. It has been crafted to address the typical concerns of corporate procurement and legal teams while also protecting the interests of both parties. Key features of our MSA include: definitions of the services and hardware being provided; licensing terms for the software (usually a subscription or purchase with maintenance model, clearly delineating your rights to use the software and receive updates); confidentiality clauses to ensure we keep your data and information confidential (and vice versa, you protect any Tekle confidential info); intellectual property clauses (Tekle retains IP in its products, but you retain ownership of your proprietary data and any custom content you develop – and we don't get rights to that aside from what's needed to operate the service); warranty terms (we warrant that our products will perform as described and that we will fix or replace any that do not, within certain limits and timeframes); **liability limitations** (like most tech vendors, we ask to limit liability to a certain cap except in special cases, to keep risk manageable for both parties); and termination conditions (how either party can terminate the agreement, and what happens to data and licenses upon termination). The MSA also references other documents like the DPA or SLA as part of the overall agreement. We understand some clients have specific language they need (for example, around intellectual property or compliance), and while we have a robust standard MSA, we are willing to negotiate reasonable modifications to meet your

requirements. Our goal is to reach a fair, transparent agreement so that both parties have a clear understanding of responsibilities and expectations.

Data Processing Addendum (DPA): As discussed in the privacy section, the DPA is an attachment to the MSA that specifically focuses on personal data handling and GDPR (and similar laws) compliance. Our standard DPA affirms that: we (the processor) will only process personal data on instructions from you (the controller); we have appropriate security measures (technical and organizational) in place to protect the data (essentially summarizing what we've described in this document); we will assist you in fulfilling obligations to data subjects (like if you need to notify someone of a breach, we'll give you the info you need); we will notify you promptly of any personal data breach on our side; we will delete or return personal data at end of contract as you prefer; we submit to audits/inspections by you or an agreed auditor to verify our GDPR compliance (some clients exercise this right through questionnaires or on-site visits, which we accommodate as reasonable); and we list our sub-processors with their purposes (and commit to notifying you of any intended changes to sub-processors, giving you a chance to object). We also include the EU Standard Contractual Clauses as needed for international transfers, with Tekle as the data importer and our client as data exporter, to ensure lawful cross-border data flow. For U.K. clients, we have the UK Addendum to those clauses, and for Swiss data we incorporate the necessary provisions too. Essentially, our DPA is designed to give your privacy office full confidence that using Tekle's solution will not put you out of compliance with GDPR or other data protection regimes.

Service Level Agreement (SLA): Tekle's SLA sets the performance and support standards you can expect. We typically guarantee a certain **uptime** for our cloud services – for example, an SLA might state 99.5% uptime per calendar month for the core service (not counting scheduled maintenance windows, which we keep minimal and preferably during off-hours). If we fall below that due to issues under our control, the SLA outlines remedies (often in the form of service credits). For support responsiveness, our SLA defines **support tiers and response times**: e.g., for a "Critical" issue where the system is down, we might commit to responding within 1 hour and working continuously until resolved; for a "High" priority issue (major functionality impaired), respond within 4 business hours; for "Normal" priority (general questions or minor issues), respond within 1 business day. The SLA will also clarify support hours (Tekle provides standard support during regional business hours and 24/7 emergency support for critical issues; extended 24/7 coverage for all issues can be arranged for those who need it, usually as part of a premium support plan). We pride ourselves on responsive support – our support engineers are intimately familiar with our products and aim to resolve issues efficiently, often far faster than the SLA requires. The SLA document also touches on maintenance notifications (we notify admins ahead of any planned maintenance or updates, especially for cloud systems) and backup policies (so you know data durability is managed, e.g., we backup cloud data at least daily with 30-day retention, etc.).

For on-prem deployments, the SLA focuses more on support response since uptime is in the client's hands, but we commit to helping restore functionality if something goes wrong.

Support Services: In parallel to contractual SLAs, Tekle offers a range of support and customer success services. When you first come on board, our team will typically provide **onboarding assistance** – this can include on-site installation help, training sessions for your IT and end-users, and consultation on how to integrate Tekle into your workflow effectively. We often create custom onboarding plans for larger deployments (for instance, a phased rollout across departments, with feedback loops). After deployment, our support portal is your main contact point. You can file tickets, track their progress, and access a knowledge base of articles (guides, troubleshooting tips, FAQs). We maintain an updated **documentation library** covering user guides, admin manuals, and developer docs (for the SDK), available through the Resources page or support site.

For critical operations, we offer an **Emergency Hotline** that customers can call outside of normal hours if they experience a major incident (the number and procedure is provided in the SLA and onboarding kit). This hotline connects you to an on-call Tekle engineer who can begin immediate triage. We also utilize remote support tools (with your permission) to securely view device diagnostics or server logs to expedite issue resolution. All support sessions are done in coordination with your authorized contacts to ensure security (e.g., we might ask you to enable a temporary support access mode on a device for us to see its status, and you can watch or revoke at any time).

Customer Success and Feedback: Tekle's relationship with clients is not just reactive (fixing issues) but proactive. Our customer success managers periodically check in with your team to ensure the solution is delivering value and to inform you of any new features or updates. We gather feedback and feature requests, many of which shape our roadmap. We also are happy to assist if you plan expansions or upgrades – our team can do health checks on your current deployment and advise on scaling up or integrating new modules.

Enterprise Alignment: We understand that large enterprises often have unique processes – you might need us to use a specific ticketing system, or follow a change management protocol to deploy an update in your environment. Tekle is flexible and willing to align with your needs. For example, for one large engineering firm, we provided a dedicated technical account manager who attended their quarterly review meetings and helped with forward planning of updates to fit their change freeze calendars.

For another defense client, we underwent their vendor accreditation process which included facility security clearance and personnel vetting, to be allowed to work on-site – we successfully complied, demonstrating our adaptability to such requirements.

In terms of legal compliance, our procurement support extends to things like providing **Certificates of Insurance** if your procurement requires certain insurance coverage (we carry liability and cyber insurance that meets typical thresholds), agreeing to reasonable confidentiality or ethics clauses (we abide by anti-corruption laws and can sign attestations to that effect), and adhering to Supplier Codes of Conduct if you have them (Tekle has its own ethical code that aligns well with most companies' expectations around labor practices, environmental responsibility, etc.).

Finally, all these support and procurement measures are aimed at one outcome: **your peace of mind**. When you choose Tekle, you're not just buying a piece of hardware or installing some software – you're entering a partnership with a company that is dedicated to your success and security. We stand by our system's performance, we respond when you need help, and we are transparent and accountable through formal agreements. Our hope is that this proactive stance turns procurement and deployment from a potential hurdle into a smooth journey, allowing you to focus on the transformative results of holographic technology in your business, while we handle the underlying trust and security foundations.

Conclusion:

Trust is earned, and Tekle Holographics works tirelessly to earn and maintain the trust of our enterprise customers. From ensuring compliance with laws and regulations, to architecting our technology with security at the forefront, to responding quickly when issues arise, to supporting you every step of the way – we have built our company ethos around reliability and integrity. This Trust & Security Center Overview has provided a comprehensive look at those efforts. In the rapidly evolving landscape of immersive technology, we understand that adopting new tools can be daunting for IT and security teams. That's why Tekle aims to be an open book about our practices and to continuously update them as new threats and requirements emerge. We invite you to review our detailed documentation (referenced throughout this paper and available on our Resources page) and discuss with our team any further questions or needs you might have. We are confident that our approach not only meets today's standards but is agile enough to adapt to tomorrow's challenges. By choosing Tekle Holographics, you are choosing a partner that values your trust as highly as your business – and we will never take either for granted.