📢 PLATFORM OVERVIEW & ARCHITECTURAL DECLARATION

This **Official Platform Technical Specifications & Architectural Guide** details the native capabilities, architectural design, security baselines, and operational workflows of the **IMTLazarus Education Cloud Platform**. Engineered specifically for K-12 school districts, ministries of education, and large enterprise educational hierarchies, IMTLazarus delivers unified multi-OS endpoint management, real-time hardware inventory, persistent cross-browser web filtering, AI-powered offline safeguarding, classroom digital wellness controls, and multi-tenant organizational hierarchy governance within a single cloud-native solution.

SECTION 1: ARCHITECTURAL FOUNDATION & ENTERPRISE CORE CAPABILITIES

CORE PLATFORM

1.1 Universal Multi-OS Centralization & Unified Inventory

NATIVE SUPPORT

- **Universal Multi-OS Centralization:** IMTLazarus centralizes the enrollment, monitoring, governance, and policy management of institutional ICT devices across all organizational tiers (central headquarters, regional divisions, districts, and individual schools), delivering comprehensive, native support across **Windows, macOS, ChromeOS, Android, iOS, and iPadOS**.
- **Unified Real-Time Inventory:** The platform establishes an automated, real-time asset visibility system supporting institutional accountability, audit readiness, and hardware lifecycle tracking.
- **Standardized Security Baselines:** IMTLazarus enforces standardized configuration policies, mandatory operating system security baselines, full-disk encryption, and granular access controls to guarantee device integrity across diverse school networks.
- **Persistent Online Safety & Content Filtering:** The platform delivers persistent, OS-level, policy-driven web filtering and online safeguarding controls that protect learners, teachers, and personnel across all web browsers and network environments.

1.2 Automated Lifecycle Management & Manufacturer Standards

ENTERPRISE GRADE

- **Automated Zero-Downtime Patching:** IMTLazarus automates the silent deployment of software updates, operating system patches, and security configurations in the background, maintaining consistent device performance while eliminating operational overhead for IT coordinators.
- **Remote Security & Asset Safeguarding:** Authorized administrators can execute instantaneous remote security commands—including screen lock, high-accuracy GPS/network location tracking, and selective or full remote wipe—to safeguard institutional property and sensitive educational data.
- **Actionable Executive Analytics:** The system generates actionable, role-based analytical dashboards and exportable reports to support data-driven curriculum planning, infrastructure monitoring, and future hardware expenditure.
- **Manufacturer Experience & Technical Escalation:**
  - *Decade of Enterprise Excellence:* IMTLazarus has over a decade of verified global experience designing, deploying, and maintaining enterprise-grade IT management and educational safeguarding platforms.
  - *Direct Engineering Escalation:* The platform architecture provides direct technical escalation pathways from local institutional administrators to core IMTLazarus platform engineers and Level-3 support specialists.
  - *Strict Data Privacy Compliance:* IMTLazarus guarantees full compliance with major international and local data protection laws, including GDPR and COPPA.

SECTION 2: NETWORK RESILIENCE & CARRIER NEUTRALITY

AGNOSTIC OPERATION

2.1 Standard Internet Management & Bandwidth Optimization

ZERO HARDWARE REQUIRED

- **Management Over Standard Internet:** IMTLazarus securely manages and communicates with all enrolled devices over standard, public internet connectivity without requiring specialized leased lines, private networks, or proprietary hardware appliances.
- **Zero Fixed Network Prescriptions:** The platform operates seamlessly across any network architecture, public fiber connection, cellular data allocation, satellite link, or local school Wi-Fi network without prescribing fixed connectivity methods or imposing per-device bandwidth caps. Endpoint communication protocols utilize highly compressed micro-payloads and delta-sync algorithms to ensure reliable policy enforcement even in remote or low-bandwidth locations.

2.2 Telecommunications & ISP Independence

CARRIER NEUTRAL

- **Total Carrier & ISP Neutrality:** The IMTLazarus Cloud Platform and endpoint agents are completely independent of any single telecommunications provider, internet service provider (ISP), or cellular carrier. Devices transition dynamically between wired LANs, wireless access points, regional ISP networks, and multi-carrier cellular mobile data networks without loss of management visibility, policy enforcement, or safeguarding protection.

SECTION 3: DEVICE LIFECYCLE PROVISIONING & CONFIGURATION MANAGEMENT

FULL LIFECYCLE

3.1 Multi-Platform Zero-Touch & Bulk Provisioning

AUTOMATED ONBOARDING

- **Centralized Platform Enrollment Mechanisms:** IMTLazarus provides out-of-the-box, native integration with all official OEM Platform Enrollment Mechanisms across supported operating systems, enabling automated, zero-touch bulk provisioning for institutional fleets:
  - *Apple Ecosystem (macOS, iOS, iPadOS):* Direct integration with **Apple School Manager (ASM)** and **Automated Device Enrollment (ADE/DEP)** for mandatory, over-the-air, supervised device enrollment.
  - *Windows Ecosystem (Windows 10/11):* Full support for **Windows Autopilot**, Microsoft Entra ID join, and bulk provisioning packages (`.PPKG`) for automated out-of-box setup.
  - *Android Ecosystem:* Native **Android Enterprise** integration supporting Zero-Touch Enrollment (ZTE), Fully Managed Device (Device Owner) mode, and Dedicated Device (Kiosk) configurations.
  - *ChromeOS Ecosystem:* Direct API integration and synchronization with **Google Admin Console / ChromeOS Education Upgrade** for unified Chromebook governance.
- **Manual, QR-Code & Assisted Workflows:** For legacy hardware, donated devices, or non-automated environments, IMTLazarus provides versatile manual, QR-code-based, URL-based, and technician-assisted onboarding workflows that allow rapid enrollment by site coordinators without specialized server infrastructure.
- **Shared-Device & Multi-User Login Architectures:** Engineered specifically for classroom device pools, computer laboratories, and library carts, IMTLazarus fully supports shared-device and multi-user login architectures. Upon individual student authentication, the platform dynamically applies customized user-level policies, content restrictions, and drive mappings, automatically clearing personal session data and browsing histories upon logout.
- **Enterprise Identity Federation:** The enrollment workflow integrates directly with major educational identity systems (including Google Workspace for Education and Microsoft Azure Entra ID). Upon enrollment or user login, IMTLazarus automatically reads directory attributes to assign the device and user to the correct school, organizational unit (OU), grade level, and security policy.

3.2 Dynamic Policy Engine & BAEC Equivalency Architecture

BAEC SUPPORTED

- **Baseline Configuration Profiles:** Central administrators can create, deploy, and enforce standardized baseline configuration profiles across all devices simultaneously, establishing immediate governance over security settings, Wi-Fi connectivity, enterprise certificates, and web filtering foundations.
- **Dynamic & Conditional Policy Engine:** The platform features an advanced conditional policy engine that dynamically assigns, modifies, or elevates configuration profiles based on real-time device compliance posture, network location, organizational unit, grade level, and authenticated user role.
- **Full Functional Coverage Across All Supported OSes:** IMTLazarus delivers comprehensive functional coverage for enrollment, configuration, restrictions, reporting, filtering, safeguarding, and security across **Windows, macOS, ChromeOS, Android, iOS, and iPadOS**.
- **Best Available Equivalent Capability (BAEC):** Where strict feature-for-feature parity is not technically feasible due to official OS, OEM, or API platform limitations (e.g., Apple iOS sandboxing vs. Windows kernel-level access), IMTLazarus transparently implements the **Best Available Equivalent Capability (BAEC)**. The platform achieves intended enterprise governance and security outcomes through officially supported vendor channels without violating licensing rules, bypassing OEM restrictions, or jailbreaking devices.
- **Automated Compliance Monitoring & Remediation:** Enrolled devices are continuously monitored against enterprise compliance baselines (e.g., passcode complexity, encryption status, OS patch level, agent integrity). When a device falls out of compliance, IMTLazarus automatically triggers immediate remediation workflows—such as restricting network access, blocking applications, pushing warning notifications, or initiating quarantine protocols—until compliance is restored.

SECTION 4: GRANULAR RESTRICTIONS, APPLICATION GOVERNANCE & SECURITY

ZERO-TRUST SECURITY

4.1 Context-Aware Rules, Geofencing & Hardware Restrictions

GRANULAR CONTROL

- **Time-Based & Location-Aware Rules / Geofencing:** Administrators can enforce context-aware policies that adjust restrictions based on time of day (school hours vs. evenings/weekends) and physical location (in-school Wi-Fi/geofence vs. off-campus usage), where supported by the underlying OS and device hardware.
- **Hierarchy-Based Policy Inheritance & Protection:** IMTLazarus enforces strict hierarchical policy inheritance. Baseline security, safeguarding, and web-filtering rules established by central administration are locked and inherited across all subordinate tiers (regional, district, and school levels), preventing local or subordinate administrators from modifying, overriding, or disabling mandatory central controls.
- **Granular Hardware & Peripheral Restrictions:** The platform provides granular administrative control to disable or restrict hardware features, including cameras, microphones, Bluetooth radios, external USB storage ports, screen capture/screenshot capabilities, AirDrop/file sharing, and factory reset functions.
- **Network Security & Access Restrictions:** IMTLazarus enforces secure network profiles by pushing mandatory Wi-Fi configurations, deploying mandatory Virtual Private Network (VPN) / proxy profiles for traffic routing, preventing connection to unauthorized or open public Wi-Fi networks, and disabling personal mobile hotspots/tethering.

4.2 Application Lifecycle Governance & Digital Wellness

APP MANAGEMENT

- **Platform-Integrated App Deployment:** Application distribution is managed natively through official platform channels, including Apple Volume Purchase Program (VPP / ASM), Managed Google Play Store for Android, Microsoft Store / Winget for Windows, and Google Workspace App Management for ChromeOS.
- **Silent Deployment, Removal & Version Enforcement:** IMTLazarus forces silent, automatic background installation, uninstallation, and updates of approved educational software without end-user intervention, enforcing mandatory minimum version requirements to ensure all endpoints operate on standardized, patched builds.
- **Allowlists, Blocklists & Transaction Blocking:** Enforcing strict application allowlists (only approved learning apps can run) and blocklists (prohibiting gaming, social media, or unauthorized tools). To prevent financial transactions and distractions, the platform natively blocks all in-app purchases, commercial app store browsing, and micro-transactional features.
- **Screen-Time & Digital Wellness:** Implementing daily app usage limits, scheduled lockout windows, and digital wellness controls to promote healthy study habits (subject to OS platform capabilities).

4.3 Endpoint Defense, Encryption & Tamper Shielding

SYSTEM SHIELDING

- **Remote Security Actions — Lock, Wipe & Lost Mode:** In the event of device theft, loss, or unauthorized reassignment, authorized administrators can instantly execute remote security commands from the central console:
  - *Remote Lock:* Immediately locking the screen with a custom institutional notification and contact phone number.
  - *Lost Mode Activation:* Activating high-accuracy GPS/network location tracking, sounding an audible alarm (even on silent), and disabling local user access.
  - *Selective / Full Remote Wipe:* Sanitizing institutional data or restoring the device to factory settings to prevent data breaches.
- **Mandatory Security Posture & Encryption Enforcement:** IMTLazarus enforces rigorous OS-level security baselines, requiring mandatory alphanumeric passcodes, configuring biometric authentication (where approved), and verifying full-disk encryption (enforcing BitLocker on Windows, FileVault on macOS, and native device encryption on Android/iOS/ChromeOS).
- **System Modification & Developer Shielding:** The platform protects operating system integrity by strictly disabling developer mode, USB debugging, command-prompt/terminal access, sideloading of unauthorized APKs/executables, and unauthorized firmware modifications or jailbreaking/rooting attempts.
- **Standardized Network & Proxy Configuration:** IMTLazarus automatically provisions standardized, encrypted Wi-Fi WPA2/WPA3 enterprise certificates, secure web proxies, and DNS rules in strict compliance with enterprise cybersecurity standards.

4.4 Continuous Real-Time Inventory & Tamper-Evident Audit Logging

LIVE TELEMETRY

- **Continuous Real-Time Inventory:** The IMTLazarus platform maintains a live, comprehensive hardware and software asset repository across the entire endpoint fleet. The inventory continuously captures unique hardware identifiers (serial numbers, MAC addresses, IMEI/MEID, UUID), OS and firmware builds, installed application lists, disk/battery health metrics, assigned users, physical locations, and chronological configuration histories.
- **Automated Security & Lifecycle Alerts:** The system generates automated, real-time administrative notifications and dashboard alerts for critical operational events, including instant alerting when newly detected devices join the tenant, or upon detection of high-risk actions such as SIM card removal, repeated failed passcode attempts, encryption deactivation, MDM profile removal attempts, or geofence boundary violations.
- **Tamper-Evident Audit Logging:** IMTLazarus generates immutable, tamper-evident administrative audit logs capturing every configuration change, policy modification, remote security command, administrative login, and compliance enforcement action, complete with UTC timestamps, IP addresses, and administrator identity.
- **Exportable Asset Reports & API Integration:** All inventory data, hardware metrics, and audit logs are readily exportable via the web console in standard formats (CSV, PDF, JSON) and are accessible via secure RESTful APIs to synchronize with institutional asset-management and ticketing systems.

SECTION 5: PERSISTENT WEB FILTERING & ONLINE SAFETY ARCHITECTURE

WEB PROTECTION

5.1 OS-Level Cross-Browser Enforcement & Circumvention Prevention

OS-LEVEL ENGINE

- **Full OS & Cross-Platform Functional Coverage:** IMTLazarus delivers complete functional coverage for web filtering and online safeguarding across Windows, macOS, ChromeOS, Android, iOS, and iPadOS, subject to official platform capabilities.
- **Persistent Cross-Browser Enforcement:** Unlike superficial filtering tools that operate only within a single specialized browser, IMTLazarus implements deep, OS-level network filtering and DNS/proxy redirection. Content filtering rules remain persistently active across **all web browsers** (Chrome, Edge, Safari, Firefox), embedded in-app browsers, and web-view components.
- **Blocking Alternative Channels & VPN/Proxy Bypass:** IMTLazarus strictly prevents user circumvention by automatically blocking unauthorized third-party browsers, anonymous proxies, Tor networks, external VPN applications, DoH (DNS over HTTPS) bypass attempts, and portable web browsers. SafeSearch-only or single-browser filtering is explicitly rejected; IMTLazarus guarantees comprehensive, tamper-proof bypass prevention across the entire operating system.

5.2 Multi-Layered Categorization & SafeSearch Governance

CATEGORIES (107)

- **Curated Education Categories:** The platform features an extensive web-filtering database containing education-curated categories (e.g., adult content, violence, gambling, malware, academic cheating, social media, streaming), maintained through continuous automated web crawling and expert human review.
- **Custom Curricular & Safeguarding Categories:** Institutional curriculum teams and safeguarding officers can create custom URL allowlists, blocklists, and specialized category groups tailored to specific subjects, research projects, or safeguarding priorities.
- **Authenticated Identity & Group-Based Scoping:** Web filtering policies dynamically apply based on authenticated user identity and organizational group membership (e.g., primary school learners receive stricter filtering than senior high school students or faculty members), ensuring age-appropriate digital access.
- **Multi-Layered Filtering Engine:** IMTLazarus combines category-based database matching, exact URL/domain filtering, and real-time keyword/page-content analysis. Any unknown, newly registered, or uncategorized URL is automatically quarantined or blocked by default until real-time AI classification or human review confirms its safety.
- **Universal SafeSearch & Thumbnail Interception:** The platform enforces mandatory SafeSearch parameters across all major search engines (Google, Bing, Yahoo, YouTube) and intercepts image search results to filter out inappropriate image thumbnails before they render on screen.

5.3 Granular YouTube Governance & Protective Review Tools

ML VIDEO FILTER

- **Granular YouTube & Streaming Media Controls:** Recognizing the educational value and potential distraction of video streaming, IMTLazarus provides granular YouTube governance:
  - *ML-Based Video Classification:* Real-time machine learning analysis of video titles, descriptions, metadata, and transcripts to block harmful or non-educational videos even on allowed platforms.
  - *Channel & Video Allowlists/Blocklists:* Restricting YouTube access exclusively to approved educational channels and curated curriculum playlists.
  - *Interface Sanitization:* Automatically hiding video comment sections, recommended sidebar videos, autoplay features, and external link thumbnails to maintain a distraction-free learning environment.
- **Staff Review & Protective Visual Tools:** When borderline or triggering visual content is detected during investigations, the platform provides protective review tools—such as automatic image blurring and content-warning overlays—allowing safeguarding staff to review flagged incidents without unnecessary exposure to graphic imagery.
- **Time-Based & Context-Based Filtering:** Supports scheduled filtering profiles that differentiate between formal school hours (enforcing strict academic allowlists) and after-school/home hours (allowing broader age-appropriate research while maintaining core safeguarding and anti-malware blocks), switching automatically without user intervention based on time of day, network location, or active login role.
- **Central Rule Supremacy & Lockout Controls:** Central administrators can initiate immediate internet lockouts (pausing all web access during testing or security incidents), deploy temporary teacher-managed classroom overrides (allowing access to a specific site for a lesson), and prevent subordinate site administrators from disabling or weakening mandatory safety configurations.
- **Real-Time Alerting & Event Logging:** Generates instant real-time dashboard notifications and automated email/SMS alerts upon detecting attempted policy violations or access to high-risk web categories. Maintains detailed, searchable, exportable logs of all allowed and blocked web traffic.

SECTION 6: ACTIONABLE ANALYTICS, DASHBOARDING & HEALTH TELEMETRY

ANALYTICS ENGINE

6.1 Role-Based Dashboards & Foreground App Telemetry

EXECUTIVE VIEWS

- **Tailored Stakeholder Dashboards:** The platform console delivers role-specific executive and operational dashboards customized for distinct institutional stakeholder groups:
  - *ICT Administrators:* Focus on network health, device connectivity, agent integrity, OS patch levels, and deployment progress.
  - *Curriculum Teams:* Focus on learning application utilization, digital textbook engagement, and academic tool adoption across grade levels.
  - *Institutional Leadership:* Focus on school-level device activity, student digital engagement, attendance correlation, and safeguarding alerts.
  - *Finance & Asset Officers:* Focus on hardware inventory distribution, license utilization rates, software ROI, and warranty/asset lifecycle status.
- **Installed vs. Active Foreground Usage Capture:** Going beyond simple app inventory, IMTLazarus records granular application engagement metrics, distinguishing between applications that are merely installed versus those actively running in the foreground. Reports detail exact usage duration (minutes per day), launch frequency, and time-of-day distribution.
- **In-School vs. Off-Campus Differentiation:** Telemetry analytics automatically segregate device usage data generated within school premises (during school hours) from data generated outside school boundaries (after hours or at home), providing vital insights into digital homework adoption and connectivity needs.
- **Curriculum Correlation Reporting:** Generates specialized instructional reports showing digital tool usage aggregated by academic subject, grade level, district, and region, empowering curriculum developers to evaluate whether procured digital resources are being actively engaged to support official learning competencies.

6.2 ROI Optimization, Health Diagnostics & Privacy Governance

COST OPTIMIZATION

- **Software ROI & License Redundancy Optimization:** Analyzes institutional software usage to calculate Return on Investment (ROI), automatically highlighting zero-usage applications, redundant commercial software licenses, and underutilized digital tools, enabling organizations to optimize IT expenditure and manage license renewals effectively.
- **Network Health & Automated Speed Diagnostics:** Continuous monitoring of device connectivity states, daily operational uptime, Wi-Fi signal strength, and network data throughput. Enrolled endpoint agents can execute scheduled, background network-speed and latency tests, automatically aggregating bandwidth telemetry to identify localized network bottlenecks.
- **ML-Based Anomaly Detection & Early Warnings:** Built-in machine learning algorithms analyze historical usage trends to flag operational anomalies—such as schools with unusually low learning-app engagement, sudden spikes in offline devices, irregular data transfer patterns, or check-in failures—generating automated early-warning tickets before localized issues become systemic failures.
- **Data Privacy Governance Module:** Features a dedicated Data Privacy Governance module that tracks the developer privacy policies and data-collection permissions of all installed mobile and desktop applications, supporting structured app-approval workflows to verify child privacy compliance.
- **Open RESTful API Exchange:** Provides robust, documented RESTful APIs that enable bi-directional data integration with external institutional systems (data warehouses, ticketing tools, and asset registries), operating under industry-standard OAuth2/JWT authentication and strict data-governance controls.

SECTION 7: AI-POWERED SAFEGUARDING & STUDENT WELLBEING ENGINE

AI SAFEGUARDING

7.1 Contextual AI Risk Detection & Native Multilingual Processing

MULTILINGUAL AI

- **Contextual AI & Behavioral Risk Analysis:** IMTLazarus incorporates an advanced artificial intelligence and contextual-language processing engine that continuously scans online searches, web browsing, typed communications, and document titles on managed devices. The engine accurately detects behavioral indicators of **self-harm, suicide ideation, severe cyberbullying, physical violence, weapons, drug/substance abuse, and exposure to explicit or predatory content**.
- **Native Multilingual & Colloquial Support:** Optimized for diverse regional educational environments, the AI detection engine natively processes and analyzes text in major international languages (including English and Spanish). Furthermore, the engine supports dynamic vocabulary updates, allowing institutional safeguarding teams to input custom keywords, local terminology, or emerging slang to maintain effective monitoring.
- **Universal & Offline Safeguarding Monitoring:** Safeguarding monitoring operates continuously across all supported operating systems during online and offline activity. When a student uses a device offline, the IMTLazarus agent logs all activities, evaluates text against local safeguarding dictionaries, and instantly transmits queued risk alerts to the central console the moment network connectivity is re-established.

7.2 Case Management, Hierarchical Escalation & PII Redaction

END-TO-END SECURITY

- **Granular Sensitivity Calibration:** Authorized safeguarding officers can dynamically adjust AI detection sensitivity thresholds (e.g., Low, Medium, High, Critical) and risk categories based on student age groups, grade levels, or specific educational programs, aligning strictly with formal child-protection frameworks.
- **Automated Hierarchical Incident Routing:** When a high-severity safeguarding incident is detected (e.g., active self-harm ideation), IMTLazarus automatically routes immediate email, SMS, and dashboard alerts to designated school guidance counselors, child-protection officers, or regional safeguarding leads in accordance with defined escalation hierarchies.
- **Secure End-to-End Case Management:** Provides a secure, built-in case management module where designated officers can review incident details, record intervention notes, assign follow-up tasks, track student support actions, and formally close cases within an auditable, confidential workflow.
- **Immutable Incident Snapshots & Audit Trails:** Incident records automatically capture complete diagnostic and behavioral context—including triggering text/keywords, surrounding sentence context, exact URL/ application name, UTC timestamp, device serial number, and masked student identifier—backed by an unbroken, time-stamped audit trail.
- **Automated PII Redaction & Cryptographic Security:** To protect student privacy and prevent unauthorized disclosure, IMTLazarus automatically masks or redacts Personally Identifiable Information (PII)—such as student names, ID numbers, and profile photos—in general dashboard views and exported reports. Full PII de-anonymization is restricted exclusively to authorized officers holding specialized cryptographic permissions. All safeguarding data, risk alerts, and case notes are encrypted in transit using **TLS 1.3** and at rest using **AES-256** encryption within segregated cloud databases.

SECTION 8: HIGH AVAILABILITY ARCHITECTURE & IDENTITY FEDERATION

CLOUD SLA

8.1 Offline Policy Enforcement & Delta Synchronization

OFFLINE CACHE & SYNC

- **Persistent Offline Protection:** Content-filtering rules, device restrictions, application allowlists/blocklists, and enterprise security policies remain persistently active and enforced on managed devices even when completely disconnected from internet connectivity.
- **Native Architecture Support:** Previously deployed content-filtering rules, device policies, and applicable security or compliance controls remain actively enforced while the managed endpoint is offline, utilizing native capabilities supported by the applicable operating system (Windows, macOS, ChromeOS, Android, iOS, iPadOS), enrollment method, device configuration, Platform Enrollment Mechanism, and cloud MDM architecture.
- **Asynchronous Offline Operation:** An offline endpoint is not expected to receive new real-time administrative commands, live policy updates, or instant reporting instructions while disconnected from network infrastructure.
- **Automated Delta-Sync Upon Reconnection:** New administrative commands, policy modifications, local audit logs, usage telemetry, compliance status evaluations, safeguarding alerts, and monitoring data are automatically queued locally and synchronize, reflect, or execute the instant network connectivity is restored, utilizing resilient OS and platform delta-sync mechanisms.
- **Outcome-Based Architectural Compliance:** IMTLazarus fulfills this requirement through a robust, outcome-based architecture utilizing official OS APIs, native system daemons, and local agent policy caching, without prescribing fixed technical methods such as mandatory on-device decision engines, heavy local database caching, or proprietary hardware/offline-processing architectures.

8.2 High Availability, Fault Tolerance & Cloud-Native Scalability

99.99% CLOUD SLA

- **High Availability & Fault Tolerance:** Ensures uninterrupted operation through redundant, multi-region cloud infrastructure (AWS/GCP), automated load balancing, and failover clustering to guarantee 99.99% operational uptime across institutional deployments.
- **Central Policy Synchronization:** Maintains continuous, automated policy synchronization between endpoint device agents and central management servers using lightweight web-sockets, background push notifications, and adaptive polling.
- **Cloud-Native Scalability:** Engineered with a cloud-native microservices architecture that dynamically auto-scales compute, memory, and database ingestion resources to support nationwide institutional distribution across 1,000,000+ simultaneously managed endpoints without degradation in response time or policy enforcement speed.
- **Logging & Telemetry Reliability:** Endpoint agents utilize resilient local buffering, cryptographic check-summing, and automated exponential back-off retry protocols to guarantee the reliable, lossless delivery of audit logs, asset telemetry, and monitoring data to central institutional databases and enterprise data registries.

8.3 Enterprise Identity Federation, RBAC & Certificate PKI Authentication

ZERO-TRUST ACCESS

- **Native Identity Provider Integration:** IMTLazarus natively integrates and federates with enterprise educational identity systems, specifically **Google Workspace for Education** and **Microsoft Azure Entra ID**, supporting Single Sign-On (SSO), SAML 2.0, and OpenID Connect (OIDC) authentication for both administrators and end-users.
- **Automated Directory Synchronization:** Maintains real-time synchronization of user accounts, organizational units (OUs), security groups, and classroom rosters, ensuring that when a student or faculty member changes schools or grade levels in the central directory, their MDM policies and safeguarding profiles update automatically.
- **Multi-Tenant Hierarchical Administration & Delegation:** Features a true multi-tenant hierarchical architecture mirroring complex institutional structures—from central headquarters down to regional divisions, districts, and individual schools. Central administrators can assign granular, delegated administrative permissions (RBAC) to local IT coordinators, allowing site management while preserving mandatory central security baselines.
- **Certificate-Based Authentication & PKI:** Natively supports Public Key Infrastructure (PKI), Simple Certificate Enrollment Protocol (SCEP), and equivalent certificate-based authentication mechanisms to validate device identity and secure mutual TLS communications across public networks.

SECTION 9: LICENSING MODEL, CLOUD SECURITY & IMPLEMENTATION STANDARDS

ENTERPRISE TERMS

SPECIFICATION CATEGORY	ENTERPRISE STANDARD	IMTLAZARUS PLATFORM ARCHITECTURAL CAPABILITY & COMPLIANCE VERIFICATION
9.1 Licensing Model & Free Transferability	Per-Device Transferable Entitlements; Flexible Pool Allocation; Dynamic Sequencing.	• **Per-Device Transferable Entitlements:** IMTLazarus licenses are issued on a per-device, transferable basis. When an enrolled device is replaced, repaired, retired, or reallocated, its license entitlement can be instantly reassigned to a replacement device at no additional licensing cost. • **Flexible Central Pool Allocation:** Enterprise procurements cover unassigned central entitlement pools that are not tied to specific brands, hardware models, OS versions, or site locations prior to deployment. • **Dynamic Deployment Sequencing:** Actual device distribution and enrollment sequencing are managed dynamically during implementation without restrictive brand or OS pre-allocation quotas.

SPECIFICATION CATEGORY	ENTERPRISE STANDARD	IMTLAZARUS PLATFORM ARCHITECTURAL CAPABILITY & COMPLIANCE VERIFICATION
9.2 Subscription Terms & Onboarding Flexibility	Common Subscription Terms; Onboarding Grace Periods; Zero Rollout Surcharges.	• **Common Subscription Terms:** Large-scale enterprise allocations share unified common subscription terms with synchronized commencement and expiration dates across the estate. • **Onboarding Grace Period Support:** IMTLazarus natively accommodates structured onboarding grace periods (e.g., 60 calendar days) for tenant provisioning, baseline configuration, identity federation, and initial batch enrollment demonstrations prior to formal term commencement. • **Zero Rollout Surcharges:** Platform access, license entitlements, technical support, and onboarding services during designated implementation grace periods are fully supported without separate surcharges or platform fee penalties.
9.3 Administrative Access & Cloud Security Certifications	Unlimited Administrative RBAC Accounts; ISO/IEC 27001 & SOC 2 Type II Infrastructure.	• **Unlimited Administrative Accounts:** IMTLazarus provides administrative accounts across all institutional tiers (central headquarters, regional offices, districts, and school sites) at no additional cost, supporting granular Role-Based Access Control (RBAC). • **ISO/IEC 27001 & SOC 2 Type II Certification:** Hosted within secure cloud environments covered by current, valid ISO/IEC 27001 and SOC 2 Type II international security certifications.
9.4 Included Maintenance, Data Ownership & Portability	Included Updates & Patches; Non-Proprietary Data Export; Exit Portability.	• **Included Maintenance & Upgrades:** All maintenance releases, software patches, version upgrades, and new feature updates released during the subscription term are provided across the entire managed estate at no additional cost. No future premium modules or separate license fees are required to maintain core platform compliance. • **Full Data Ownership & Free Exportability:** Institutional clients retain absolute ownership and export rights over all device inventories, audit logs, and safeguarding analytics. All data can be exported on demand in non-proprietary formats (CSV, PDF, JSON) without export fees. • **Continuity & Exit Portability:** At contract expiration or transition, IMTLazarus provides human-readable documentation, policy templates, and exportable data archives to support seamless transition planning without restricting operational data access.

SPECIFICATION CATEGORY	ENTERPRISE STANDARD	IMTLAZARUS PLATFORM ARCHITECTURAL CAPABILITY & COMPLIANCE VERIFICATION
9.5 Turnkey Architecture, Zero Downtime & Blended Training	Unified Single Tenant; Zero-Downtime Silent Updates; Nationwide Blended Training.	• **Turnkey Single-Tenant Architecture:** Delivered as a complete, unified cloud solution under one single institutional tenant, eliminating fragmented regional or brand-specific portal instances while supporting delegated multi-level hierarchies. • **Zero-Downtime Deployment & Rollback:** All platform updates and policy configurations deploy silently in the background without system downtime or classroom operational disruption, supported by automated console rollback procedures. • **Comprehensive Blended Training Curriculum:** Accommodates nationwide train-the-trainer programs combining instructor-led hands-on workshops, self-paced online certification modules, and recurring technical refresher sessions, with full internal use and reproduction rights turned over to the organization.