Scaling Secure Digital Learning

Bridging the Digital Divide with Unified Governance

Powered by IMTLazarus

Transforming ICT Assets into a Governed Ecosystem

Objective 1: Unbreakable Security

Establishing unbreakable, root-level security baselines nationwide. By binding policies to the hardware level, DepEd ensures that every managed device adheres to centralized safety standards.

Crucially, these policies apply regardless of the Operating System and cannot be bypassed by local modifications or factory resets by end-users.

Objective 2: 100% Transparency

Achieving absolute transparency across the entire fleet. This provides the Central Office with instant, actionable data on hardware identifiers, compliance status, and geographic distribution.

This level of visibility is mandatory to satisfy the rigorous accountability and audit requirements

2. Architectural Superiority

Engineering for hundreds of thousands of nodes

Traditional MDM architectures fail because they rely on localized server infrastructures. These "local" models create enormous bottlenecks and single points of failure.

- **Cloud-Native Infrastructure:** Moves processing to the edge, eliminating the need for local imaging.
- **Military-Grade Datacenters:** Instantly synchronize hundreds of miles of simultaneous active nodes.
- **Remote Resilience:** Operates seamlessly despite intermittent connectivity and limited IT staff in remote divisions.

Comparative Technical Advantage

Feature	Traditional MDM Bottlenecks	IMTLazarus Cloud-Native Advantages
Scalability	Limited by local server capacity and divisional bandwidth.	Engineering for hundreds of thousands of nodes; horizontally scalable.
Policy Deployment	Delayed sync; often requires manual "touch" or local imaging.	Instant nationwide updates; policies push via native vendor APIs.
Infrastructure	High TCO due to hardware maintenance in remote divisions.	Zero local server footprint; latency-optimized local filtering decisions.
Connectivity	Centralized bottlenecks; updates fail during peak traffic.	Cloud-native distribution ensures 99.9% availability regardless of location.

Security Posture and Privacy Standards

ISO 27001 & SOC 2

Infrastructure hosted in military-grade datacenters with rigorous annual audits to ensure operational integrity and 99.9% infrastructure availability.

Data Privacy Act

Full alignment with Philippine National Privacy Commission standards (RA 10173) for the absolute protection of personal student information.

GDPR Alignment

Strict "Privacy by Design" ensures zero student data is ever monetized. Behavioral telemetry is encrypted natively at the edge.

3. The Administrative Hierarchy Matrix

Effective governance reflects the complexity of a tiered structure through the Nested Policy Cascade:

- **Central Ministry (Root Policy):** Establishes immutable National Safety Baselines, including unbreakable URL and App blocks that cascade downward.
- **Regional Directives:** Handles Regional Contextualization & Compliance Monitoring, ensuring local alignment with national goals.
- **Division IT Ops:** Manages Technical Mobilization & Enrollment Workflow Management for localized logistical control.
- **School-Level Management:** Provides sandboxed capabilities for Classroom-specific instructional flexibility without overriding root security.

Role-Based Operational Synergy

System Functionality	Central Ministry & IT Admins	Classroom Teachers
Global Policy Control	Establishes root-level security bound to device hardware.	Operates within pre-approved parameters; cannot override central security.
App & URL Management	Manages master whitelists/blacklists and permanent VPN blocks.	Can temporarily unlock specific educational URLs for a 45-minute class session.
Student Monitoring	Full access to automated telemetry and national risk logging.	Real-time visibility into student screen activity during active sessions.

4. Advanced Safeguarding

The "See the Signs" Protocol

Digital learning requires active protection based on artificial intelligence, aligned with the Child Protection Policy.

- **Closing the Crisis Gap:** AI-driven detection scans for indicators of self-harm, radicalization, and cyberbullying, accelerating counselor intervention.
- **Linguistic Mastery:** Preconfigured for regional terminologies.
- **Contextual Sensitivity:** Detection sensitivity adjusts by age group and risk category, evolving as the student matures.

Network-Level Persistence & DNS Protection

Client-side extensions are easily disabled. IMTLazarus utilizes unbreakable network-level protocols:

Anti-Bypass Protocols

Filtering operates independently of the browser, preventing circumvention via rogue VPNs, proxy tunnels, or embedded web-views.

DNS-Layer Protection

Extends protection to unmanaged and BYOD units connecting to the school network, ensuring the campus remains a safe "sandbox."

Off-Campus Continuity

Security policies remain active and apply 100% whether the student is connected to the school network or a home Wi-Fi connection.

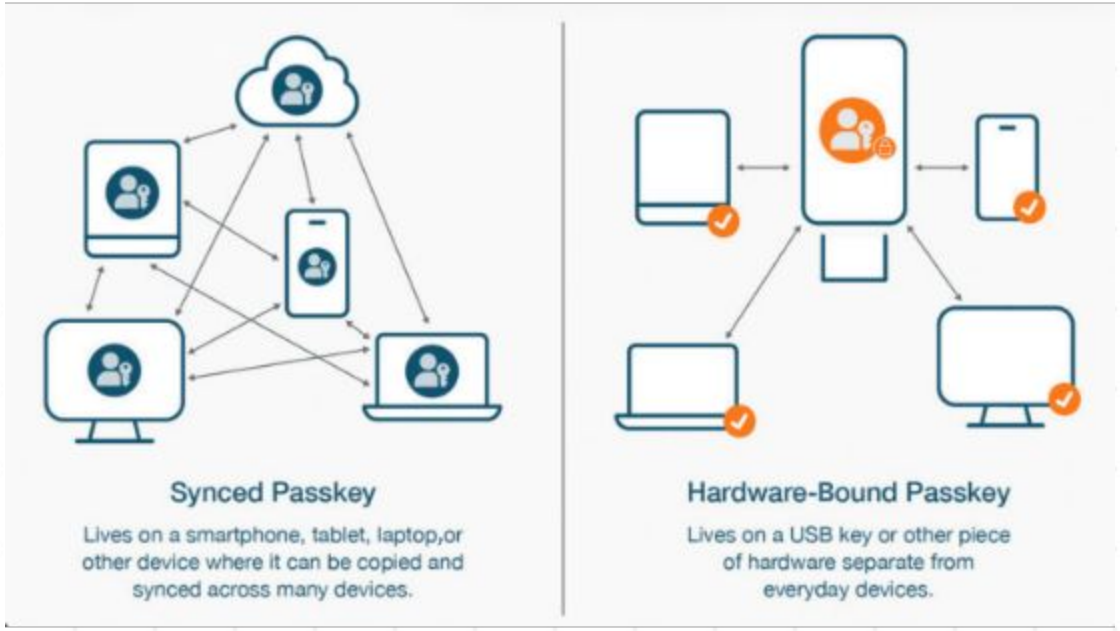
5. Zero-Touch & Multi-OS Parity

Operational Deployment

To meet delivery deadlines for hundreds of thousands of licenses, we use the "Zero-Touch" implementation, which automates configuration on first boot.

Absolute Hardware Lockdowns via Native APIs:

- **Peripheral Control:** Remotely disable cameras, Bluetooth, and USB transfers.
- **Integrity Protection:** Prevent factory resets and rogue sideloading of unauthorized APKs.
- **Deployment Flow:** Automated setup across Windows, macOS, ChromeOS, Android, and iOS.



License Transferability and TCO

Key differentiating factor for maximizing investment:

Maximizing Investment Lifecycle

Unlike traditional MDMs where a license is "burned" to a single device, IMTLazarus licenses are fully transferable.
If a device is decommissioned or sent for repair, the license is easily reassigned to the replacement unit at no additional cost.

Deferred Consumption

The 12-month subscription lifecycle begins only upon explicit assignment and activation to a device.

This ensures the government budget is optimized and not wasted on hardware sitting idle in regional warehouses.

6. Service Level Excellence

Severity Level	Definition	Response Time	Resolution Time
1 - Critical	Platform outage, security breach, or failure of safeguarding alerts.	Within 1 Hour	Within 4 Hours
2 - High	Major function degradation or filtering update failures.	Within 2 Hours	Within 12 Hours
3 - Moderate	Issues affecting a limited number of devices or minor inaccuracies.	Within 4 Hours	Within 48 Hours
4 - Low	General inquiries or documentation-related concerns.	1 Business Day	3 Business Days

Vendor Accountability: Failure to resolve Severity 1 incidents yields a penalty of 0.1% of MEV per hour. Cumulative uptime below 95% triggers a mandatory review and a 20% service credit.

7. Implementation Roadmap

Mobilize hundreds of thousands of licenses through four high-precision milestones:

1. Initiation

System mobilization, tenant activation, identity integration (Google/Azure), and hierarchy establishment.

2. Configuration

Development of security baselines and content filtering. Rigorous UAT with 100% pass-rate required.

3. Enrollment

Nationwide "Train-the-Trainer" program launch and activation of the Online Learning Portal for certification.

4. Turnover

Delivery of "as-built" documentation, architecture diagrams, and transition of administrative credentials.

IMTLazarus AI: Beyond Traditional Filtering

Next-Generation Safeguarding

Proactive Risk Detection: Utilizing advanced Natural Language Processing (NLP) to detect nuanced indicators of cyberbullying, self-harm, and radicalization.

Linguistic Mastery: Engineered to understand complex code-switching, regional dialects, and modern digital slang in real-time.

Zero-Day Threat Prevention: Dynamic categorization instantly evaluates and blocks previously unseen malicious URLs before they reach the student.

Behavioral Analytics: Provides counselors and educators with actionable insights into student engagement and digital habits.