Cybersecurity Services Catalog

Los Angeles County Office of Education

Information Systems Security
Technology Services

Los Angeles County Office of Education

Information Systems Security
Technology Services

The Information Systems Security Unit at LACOE acts as a technological backbone, protecting 1.3 million learners through a resilient digital environment. By shifting from reactive firefighting to predictive threat management, the team delivers a comprehensive ecosystem that mitigates enterprise risk and ensures educational continuity. Their mission is to safeguard institutional trust and align security with strategic goals, providing enterprise-grade protection across the county.

How We Can Help

LACOE serves as a strategic partner to help districts build robust programs to secure their organizations through a comprehensive ecosystem of foresight, governance, and rapid adaptability. **View a detailed list of our service offerings throughout this catalog.** Our support includes:

- **Phishing Awareness & Simulation:** We provide access to tools for sophisticated simulation campaigns and behavioral analysis.
- **Compliance & Insurance Readiness:** We perform targeted reviews to identify insurability gaps and ensure your institution meets the stringent cybersecurity insurance requirements.
- **Technical Security Assessments:** We deliver rigorous evaluations of network and cloud infrastructure to provide a strategic architectural review and a prioritized risk roadmap.
- **Third-Party Vendor Risk Evaluation:** We vet external vendors and partners to ensure they adhere to strict data privacy standards and security controls.

Contact Us

Ready to build a resilient security program for your organization?
We're eager to partner with you.

Email: cybersecurity@lacoe.edu
Website: lacoe.edu/cybersecurity

We look forward to collaborating with you to create a more secure and resilient digital environment for your institution.

Table of Contents

Customization

Customized Consultation Services

We offer personalized consultation to help districts build custom security programs and support structures tailored to their specific institutional needs. Our team works closely with leadership to ensure all security architectures align with industry best practices and rigorous regulatory requirements.

Delivery: LACOE

Staff Augmentation

We provide scalable, expert personnel to bridge internal skill gaps and ensure the continuous maintenance of your security systems. Our professionals integrate with your team to manage complex projects and specialized tasks, delivering high-level expertise without the burden of long-term hiring.

Delivery: LACOE

Security Awareness & Culture

Phishing Simulation

We provide a managed platform for sophisticated phishing simulations and behavioral analytics. These exercises are designed to transform staff into a vigilant human firewall, reducing the risk of successful social engineering and credential harvesting.

- Sophisticated phishing simulations that mimic real-world threats to measure and reduce user vulnerability in a safe, controlled environment.
- Delivers bite-sized, immediate training modules to users who engage with simulated phish, ensuring behavioral correction in real time
- Comprehensive dashboards that translate simulation results into measurable "Human Risk" KPIs for district leadership and insurance underwriters.

Delivery: LACOE + Platform

Los Angeles County Office of Education

Security Awareness & Culture (cont.)

Cyberscurity Training

We offer specialized curriculum and advisory services focused on identity lifecycle management, multi-factor authentication (MFA) adoption, and AI-driven threat mitigation. This ensures that users understand their role in maintaining data privacy and institutional integrity.

- **Identity & MFA Training:** Master secure credential management and multi-factor authentication to protect digital identities.
- **AI Threat Defense:** Learn to recognize and block advanced AI-driven threats like deepfakes and automated social engineering.
- **Compliance & Data Privacy:** Understand regulatory requirements and best practices for safeguarding sensitive student and district data.

Delivery: LACOE

Strategic Governance

Cybersecurity Insurance Readiness Assessment

With rising K-12 premiums, insurers now require proof of mature security controls rather than simple questionnaires. Our assessment identifies "insurability gaps" by evaluating your environment against carrier-mandated standards—like MFA, EDR, and immutable backups—to ensure a low-risk profile that secures coverage and optimizes rates.

- **Carrier-Aligned Technical Assessment:** Verify mission-critical controls and MFA coverage across all remote access and administrative systems.
- **Operational Policy & Documentation Review:** assessment, incident response, and disaster recovery plans to meet insurance and legal governance standards.
- **Remediation Roadmap:** Prioritize fixing high-severity gaps to qualify for better coverage limits and lower deductibles.

Delivery: LACOE + Partners

Los Angeles County Office of Education

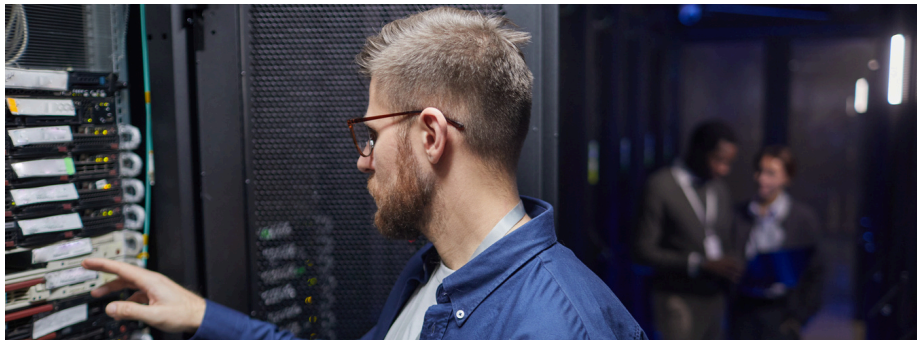
Strategic Governance (cont.)

Vendor Risk Evaluation

As school districts increasingly rely on cloud-based platforms, the "supply chain" becomes a primary vector for data breaches. Our Vendor Risk Evaluation service provides a standardized, rigorous framework for assessing the security maturity of third-party partners before they are granted access to your network or student data. We move beyond simple "check-the-box" questionnaires to provide a technical and legal analysis of how vendors handle encryption, data retention, and incident notification.

- **Security Posture & Compliance Auditing:** We analyze vendor SOC2 reports, HECVAT submissions, and privacy policies to ensure their technical controls align with California student data privacy laws (AB 1584/SOPIPA).
- **Data Flow & Interconnectivity Analysis:** Our team reviews how vendors integrate with your district's API and identity providers to prevent unauthorized data "shadowing" or insecure credential storage.
- **Continuous Vendor Monitoring & Scorecards:** We provide ongoing risk scoring for your existing vendor ecosystem, alerting you to security regressions or breaches within your supply chain as they happen.

Delivery: LACOE



Los Angeles County Office of Education

Strategic Governance (cont.)

Vulnerability Management & Governance

This comprehensive service bridges the gap between technical defense and strategic oversight. We move beyond simple scanning to build a resilient security framework that aligns your district's "Vulnerability Management" with long-term governance, policy, and recovery standards.

- **Cybersecurity Strategic Tech Planning:** We assist in drafting your Purpose, Vision, and Focus Areas, creating a multi-year roadmap that aligns security investments with educational goals. This includes defining Strategic Actions and measurable KPIs to track maturity over time.
- **Policy Development & Governance:** Our experts help draft and refine essential cybersecurity policies (AUP, Data Privacy, and Incident Handling) to ensure your district meets state and federal regulatory mandates while fostering a culture of accountability.
- **Resilience Planning (BIA, BCP, & DR):** We facilitate a Business Impact Analysis (BIA) to identify mission-critical services, then develop a Business Continuity Plan (BCP) and Disaster Recovery (DR) strategy to ensure the district can operate during and after a catastrophic failure.
- **Response Framework (IR Plan):** We assist in the creation or overhaul of your Incident Response (IR) Plan, establishing clear escalation paths, roles, and communication trees to ensure a coordinated response to cyber threats.

Delivery: LACOE + Partners

Los Angeles County Office of Education

Incident Readiness

Incident Response Excercises

We provide full-lifecycle incident management that transitions your district from reactive firefighting to a posture of resilient defense through proactive monitoring and expert-led response protocols. Our team facilitates custom tabletop exercises to stress-test your communication and decision-making workflows, ensuring leadership and IT staff are prepared for real-world ransomware or data breach scenarios. In the event of an active threat, we deliver hands-on support for forensic investigation and evidence preservation, while providing the recovery governance necessary to securely restore mission-critical educational services and satisfy insurance requirements.

- **Technical Tabletop Exercises:** These hands-on simulations challenge IT and security teams to resolve complex technical scenarios, such as active ransomware infections or privilege escalation, within their specific infrastructure.
- **Executive Tabletop Exercises** We facilitate high-level simulations for district leadership to refine communication strategies, legal obligations, and financial decision-making during a significant cyber crisis.
- **Incident Response Review**: Our team performs a comprehensive audit of your existing response plans to identify gaps in documentation and ensure workflows align with the latest NIST and CIS regulatory standards.

Delivery: LACOE + Partners

Los Angeles County Office of Education

Incident Readiness (cont.)

IR Playbook Development

While a general policy outlines what should happen, a Playbook provides the step-by-step technical and operational instructions for how to handle specific threats. We partner with your district to draft customized, "if-then" action plans for the most common K-12 threats, ensuring that when an alert triggers, your team isn't improvising.

- **Threat-Specific Action Plans** We develop granular response steps for high-probability scenarios, including ransomware, business email compromise (BEC), and unauthorized student data access.
- **Communication & Notification Trees** :Our team builds clear escalation matrices that define exactly who to call and when—from internal IT and Superintendents to external legal counsel and law enforcement.
- **Role-Based Responsibility Matrix (RACI):** We establish a clear division of labor during a crisis, ensuring that IT, Communications, and Legal departments understand their specific duties without overlap or confusion.

Delivery: LACOE

Los Angeles County Office of Education

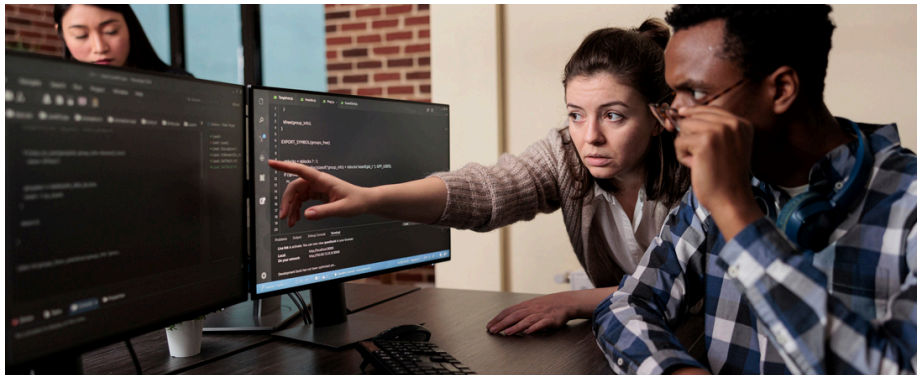
Infrastructure Security

Penetration Testing

While vulnerability scans find potential weaknesses, our penetration testing service goes a step further by safely attempting to exploit those gaps to see how far an attacker could actually get. We provide an "attacker's eye view" of your network, testing your defenses against advanced techniques like lateral movement, privilege escalation, and data exfiltration.

- **Internal and External Infrastructure Testing:** Our experts attempt to breach your network perimeter and move through internal segments to identify exactly where your security controls fail to stop an intruder.
- **Web Application & Portal Assessment:** We perform deep-dive testing of public-facing assets, such as Student Information Systems and parent portals, to identify flaws that could lead to unauthorized access or data leaks.
- **Exploitable Vulnerability Validation & Remediation:** We provide a validated report of confirmed exploits along with a prioritized roadmap to fix the most critical issues first.

Delivery: LACOE + Partners



Los Angeles County Office of Education

Infrastructure Security (cont.)

Security & Architecture Reviews

We deliver rigorous, expert-led evaluations of network design and cloud infrastructure. These assessments provide a strategic architectural review and a prioritized risk roadmap, allowing districts to identify vulnerabilities and remediate gaps before they are exploited.

- Expert evaluations of network and cloud designs to ensure alignment with industry-standard security benchmarks.
- Identify digital weaknesses to proactively remediate gaps before they can be exploited.
- Strategic architectural review that translates technical findings into a prioritized roadmap

Delivery: LACOE + Partners

Distributed Denial-of-Service (DDoS) Protection

We leverage Cloudflare's global network to provide autonomous, edge-based mitigation that identifies and blocks malicious traffic in seconds, preventing disruption to critical district operations such as online testing or enrollment. This service includes comprehensive protection for your entire IP infrastructure, with unmetered mitigation to ensure total budget predictability regardless of attack volume or frequency.

- Edge-based mitigation automatically blocks malicious traffic, ensuring online access remains accessible during high-volume attacks.
- Access to a unified dashboard that provides deep visibility into global traffic patterns and detailed logs of blocked attacks.
- Behavioral analysis and machine learning to distinguish between legitimate users and malicious bots

Delivery: LACOE + Platform

Los Angeles County Office of Education

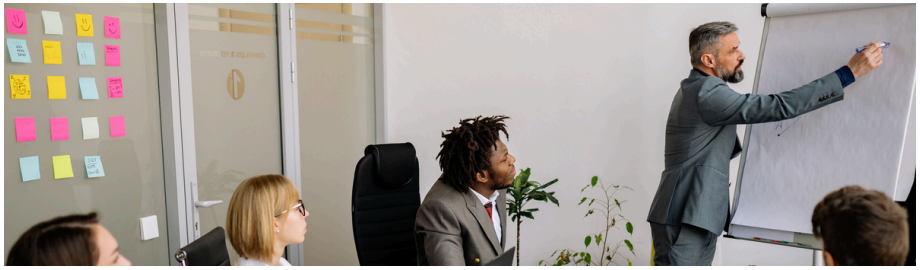
Crisis Response

Incident Response Support

When a district faces a high-pressure event—such as ransomware, data exfiltration, or a significant service outage—our Incident & Crisis Response service provides the elite technical support and governance required to contain the threat and stabilize the environment. We act as a force multiplier for your IT team, offering expert guidance to navigate the complex technical, legal, and communication challenges that arise during a crisis.

- **Emergency Containment & Threat Hunting:** We can help support districts to help isolate infected systems, sever attacker persistence, and hunt for dormant malware to prevent re-infection.
- **Forensic Investigation & Preservation:** Our team performs can perform a deep-dive analysis of logs and system artifacts to determine the "patient zero" and the scope of the breach, ensuring all evidence is preserved for legal and insurance requirements.
- **Crisis Communications & Stakeholder Management:** We assist leadership in drafting transparent, timely notifications for parents, staff, and state agencies, ensuring the district maintains trust while meeting legal disclosure mandates.
- Secure Recovery & Restoration Governance We provide a structured roadmap for restoring services, validating that backups are clean and that systems are hardened before they are brought back online to avoid a secondary attack.

Delivery: LACOE + Partners



Los Angeles County Office of Education

Technical Training

Technology Specific Training

o maintain a resilient infrastructure, district technical personnel must stay ahead of the rapidly evolving toolsets they manage. Our Vendor-Partnered Technical Training service bridges the gap between general IT knowledge and platform-specific mastery. We facilitate deep-dive, hands-on sessions led by certified engineers from our primary technology partners—such as Cloudflare, Microsoft, Cisco, and Fortinet—to ensure your team can fully leverage the advanced security and networking features of your existing investments.

- **Systems-Specific Deep Dives:** Access advanced curriculum focused on the precise configuration, optimization, and troubleshooting of your district's specific hardware and software stacks.
- **Direct Access to Vendor Engineers:** Participate in interactive workshops and "Office Hours" where your technical staff can collaborate directly with vendor architects to solve complex environmental challenges.
- **Certification & Skill Path Alignment:** We align training modules with industry-recognized certifications, helping your staff build professional equity while strengthening district defenses.

Delivery: LACOE + Partners

Los Angeles County Office of Education

Los Angeles County Office of Education

9300 Imperial Highway,
Downey, California 90242-2890
www.lacoe.edu