## Kindergarten Through 12th Grade Security Information Exchange (K12 SIX)

K12 SIX is a real-time cyber threat intelligence sharing hub exclusively for schools, to aid in preventing and mitigating cyber threats.

This non-profit member community provides cost-effective collective defense by crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security team.

## Benefits

- Engagement in a private, vetted community of 250+ (and growing) K-12 information security professionals
- Access to a secure threat information sharing platform and mobile app with actionable alerts, reports, and best practices library
- Enrollment in the K12 SIX emergency notification system for warning via phone, email, and SMS of pervasive or highly destructive attacks requiring immediate action
- Leadership, staff development, advocacy, and training opportunities through participation in K12 SIX events, committees, and advisory groups
- Discounts on select cybersecurity products and services
- Access to virtual CISO services and K12 SIX security analysts

## How It works

A school district joins the community as a member, plugging its IT team into the group via a secure sharing portal. Through the portal, the district has access to actionable intelligence and alerts generated from data submitted by other members and multiple intelligence sources accessible to K12 SIX staff. Peers in the community may contribute findings on specific malware, phishing attempts, and system vulnerabilities, and provide best practices and mitigation techniques. Members can join collaborative special interest committees to tackle industry challenges or just share their most effective policies in the portal's document repository, for community awareness. The K12 SIX staff provides in-depth threat analysis, facilitates collaboration, and integrates intelligence from partner security vendors, government sources, other sharing communities, and the Global Resilience Federation (GRF) international network of affiliates.

## Institutional Knowledge

K12 SIX is part of the Global Resilience Federation (GRF) network of threat information sharing communities, spanning many industries and thousands of organizations. GRF acts as a hub to push relevant cross-sector threat material for added awareness and resilience. Intelligence is sourced from the group, specifically for the defensive requirements of a sector, with enrichment performed by a given community's analysts.

The K12 SIX Essential Cybersecurity Protections consist of a dozen cybersecurity controls—grouped into four categories—that every school district should strive to implement:

| Recommended Protective Measure | Description |
|---|---|
| **1.0 Sanitize Network Traffic to/from the Internet** | |
| **1.1 Filter out malware** | Block access to known malicious websites |
| **1.2 Campaign against email scams** | Reduce the odds that email-based social engineering attacks succeed |
| **1.3 Block malicious documents** | Block access to malicious office suite documents, commonly responsible for ransomware |
| **1.4 Limit exposed services** | Limit internet exposure of services like remote desktop protocol (RDP) |
| **2.0 Safeguard Student, Teacher, and Staff Devices** | |
| **2.1 Restrict administrative access** | Keep devices protected and in compliance with security policies |
| **2.2 Apply endpoint protection** | Ensure devices used for school remain safe whether used on or off premises |
| **3.0 Protect the Identities of Students, Teachers, and Staff** | |
| **3.1 Protect user logins** | Implement multi-factor authentication (MFA) to safeguard against compromised passwords |
| **3.2 Improve password management** | Prevent password compromise, sharing, and re-use—commonly responsible for data breaches |
| **3.3 Stop online class invasions** | Ensure online classes can only be attended by authorized teachers and students |
| **4.0 Perform Regular Maintenance** | |
| **4.1 Install security updates** | Protect against known vulnerabilities through timely patching of IT systems, computers, and equipment |
| **4.2 Backup critical systems** | Build resilience against destructive attacks like ransomware through offline, immutable backups |
| **4.3 Manage sensitive data** | Ensure sensitive data is protected, archived, and deleted when no longer needed |

Contact info@k12six.org with any questions about K12 SIX or visit www.K12SIX.org. The community is open to members, and partners interested in funding, providing materials, security tools, or intelligence feeds. Learn more about GRF cross-sector sharing at www.GRF.org