Google Workspace & Microsoft 365
Security Checklist

10 Step Security Checklist for K-12 Schools

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Managed Methods

Google Workspace & Microsoft 365 Security Checklist

10 Step Security Checklist for K-12 Schools

Why do schools need Google Workspace & Microsoft 365 security?

K-12 schools rely on Google Workspace and Microsoft 365 apps, such as Gmail/Outlook, Drive/OneDrive, Shared Drive/SharePoint, Docs/Word, Sheets/Excel, and more. **You are using these cloud-based apps to create, store, and share vast amounts of sensitive information, but do you know how well you're securing it?**

Secure access controls, encryption, and threat detection are necessary to protect against unauthorized access, cyber threats, and compliance violations, and more. **Many K-12 IT teams mistakenly believe that Google and Microsoft are solely responsible for the security of their information. This is not true, as you are operating under a "shared responsibility" security model in your license agreement.** In short, this means that you are responsible for your local security settings, such as strong passwords, data loss prevention policies and controls, and access control configurations.

Misconfigurations pose significant security risks for K-12 schools, and are responsible for a majority of cyberattacks and data leaks districts have experienced over the past several years. **To mitigate these risks, you must regularly audit your configurations, implement best practices, use monitoring tools, and employ a zero-trust cybersecurity strategy.**

As your school district moves more information and activity to Google Workspace and/or Microsoft 365, **the perimeter security safeguards that you're used to have become less effective.** As a result, more K-12 IT teams are opting to secure student, staff, and district financial information using a zero-trust cybersecurity strategy.

This checklist helps you lay the groundwork for your zero-trust cybersecurity strategy!

Managed Methods

10 Step Security Checklist for K-12 Schools

Audit Last Completed Date:

Set Strong Password Policies

Passwords are the fundamental beginning of any good security plan. Educate your students and staff on what makes strong and weak passwords. And why password strength is so important.

Enable your system's "require a strong password" feature. You can also set minimum and maximum password lengths, password expiration, and more. If you're setting the standards for the first time, be sure to run a check of current passwords to see whose passwords are out of compliance with the new standards. You can then force a password change through your admin console.

Configure Password Settings in Google Workspace

Configure Password Settings in Microsoft 365

Make Multi-Factor Authentication Mandatory

Multi-factor authentication requires users to take a second step, after entering the correct password, to prove they have authorized access. Currently, this typically includes entering a code that is sent to their phone via SMS. It can also include phone calls, answering security questions, mobile app prompts, MFA keys, and more.

At minimum, you should require MFA for your administration staff members. Many districts are also enabling MFA for teachers and students due to the increase in criminals targeting and hijacking these accounts that are typically less protected.

Configure 2SV in Google Workspace

Configure MFA in Microsoft 365

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Managed Methods

10 Step Security Checklist for K-12 Schools

Manage 3rd Party Apps Access

OAuth makes app use convenient for end users, but it can be a little bit of a nightmare for those in charge of IT security. The proliferation of 3rd party app use in the classroom makes it difficult to stay on top of what apps have access to your district's data, what permissions are granted, and how secure the app is itself.

System admins have the ability to control what apps are allowed permissions to the district's Google and/or Microsoft accounts. This can be as simple as restricting access to risky apps, or as detailed as creating sanctioned and unsanctioned apps lists for different users, groups, or OUs.

Configure 3rd Party Apps Settings in Google Workspace

Configure 3rd Party Apps Settings in Microsoft 365

Enable Anti-Phishing Protections

Email phishing is still the most common external threat vector. And there are a myriad of tools on the market aimed at removing phishing emails from district inboxes. Unfortunately, none work with 100% accuracy.

The best option is to start with configuring your native Gmail/Outlook anti-phishing capabilities, and then layering additional safeguards and monitors on top of it when you can. Educating your users about common phishing attacks, new ones as they arise, and how to spot them is also extremely important.

Configure Anti-Phishing Settings in Google Workspace

Configure Anti-Phishing Settings in Microsoft 365

Managed Methods

10 Step Security Checklist for K-12 Schools

Turn On Unintended External Reply Warning

One of the ways you can help keep sensitive, internal information from being shared outside of your district is to enable an external reply warning. This feature also protects districts against forged emails from malicious hackers trying to gain access to internal files and information.

When the external reply warning is enabled, users receive a pop-up notification asking if they're sure they want to send to an external domain. It's important to reinforce to your colleagues why they need to pay attention to this pop-up and think twice before dismissing it.

Configure Unintended External Reply Settings in Google Workspace

Configure Unintended External Reply Settings in Microsoft 365

Set External Sharing Standards

Beyond sending emails, you should configure external sharing standards for shared calendars, drives, folders, and files. The best approach is to start with the most strict standards possible, and then open up as needed.

Files and folders containing the most sensitive information, such as student, parent, employee, and district personally identifiable information and financial information, should rarely (if ever) be configured to allow external sharing and access. This information includes social security numbers, credit card numbers, W-2s, etc.

Configure External Sharing Settings in Google Workspace

Configure External Sharing Settings in Microsoft 365

K-12 Cybersecurity & Safety Made Easy
www.managedmethods.com | (303) 415-3640

Managed Methods

10 Step Security Checklist for K-12 Schools

Set Up Message Encryption

Encryption prevents anyone other than the intended audience from viewing a message. There are a variety of 3rd party encryption tools available, but Microsoft and Google provide native encryption options (in Google's case, "Confidential Mode" which works a little differently).

Sending sensitive and/or confidential information via email should always have encryption or confidential protections enabled. It forces the recipient to authenticate that they're the intended audience and protects it from being forwarded to others. The sender can also set up an expiration date to ensure the information isn't lingering in someone's inbox into eternity.

Configure Confidential Mode Settings in Google Workspace

Configure Encryption Settings in Microsoft 365

Set Up Data Loss Prevention (DLP) Policies

DLP is a strategy for ensuring that your district's sensitive and confidential information does not leave your internal domain—whether it's accidental or malicious.

You can set up DLP policies in both Google and Microsoft. These policies help you automate rules around how information can be accessed and shared. Most policies create alerts and actions that the system can take if a DLP policy is broken. For example, if a staff member account is trying to share a spreadsheet containing social security numbers with an outside domain, the policy can be set up to automatically warn the user, break the share, or quarantine the file.

Configure DLP Settings in Google Workspace

Configure DLP Settings in Microsoft 365

CLICK TO WATCH:
FREE! Demo On-Demand

Managed Methods

10 Step Security Checklist for K-12 Schools

Enable Mobile Management

If students, faculty, and/or staff members in your district are allowed to use mobile devices to access your district's Google/Microsoft 365 apps, like email, files, and drives, you need to protect your data with mobile management.

Configure Mobile Management Settings in Google Workspace

Configure Mobile Management Settings in Microsoft 365

Run A Security Health Audit

Once you've completed this checklist, it's a good idea to run a security audit of your Google Workspace and/or Microsoft 365 environment.

An audit will check for any configuration errors, sharing risks, files containing sensitive information, and more. It's also important to run an audit on a periodic basis. Weekly and/or monthly audits and reports can be automated and provide you with detailed information into your district cybersecurity health.

Configure Security Audits in Google Workspace

Configure Security Audits in Microsoft 365

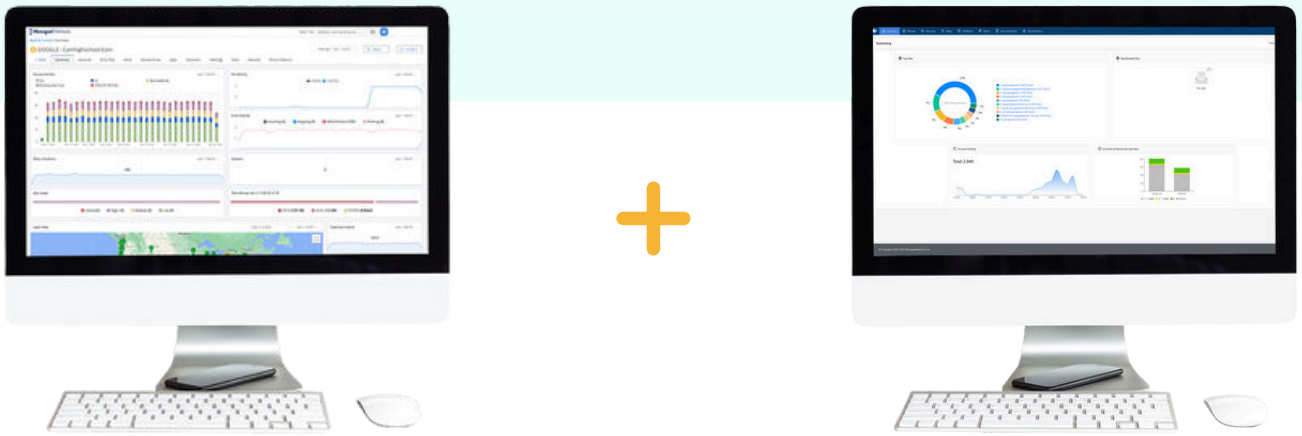
Managed Methods

Monitor | Alert | Respond

K-12 Cybersecurity & Safety Made Easy

ManagedMethods is on a mission to make online learning safer and more secure. We're the only company in the market providing K-12 specific cybersecurity and safety for Google Workspace, Microsoft 365, and in the browser.

Click Here to Claim My FREE! Security & Safety Audit



Cloud Monitor

Through automated controls, this central command center helps prevent data security breaches, account takeovers, ransomware, and phishing attacks, while also detecting student safety signals.

Problems Cloud Monitor Solves:

- Control Third-Party Apps
- Data Loss Prevention
- Phishing & Malware Threat Protection
- Prevent Account Takeovers
- Student Safety Signals

Content Filter

Light-weight, easy-to-use browser-level URL blocking and artificial intelligence to provide affordable student safety, security, and CIPA compliance for K-12 schools.

Problems Content Filter Solves:

- Easy Block & Allowlist Policies
- Customize Policies by OU
- YouTube & Social Media Blocking
- Student Safety Signals AI
- Identify Lost or Stolen Devices