Managed Methods

Cloud Security Made Easy

Cloud Application Security CHECKLIST

10 Step Cloud Application Security Checklist for Google Workspace & Microsoft 365

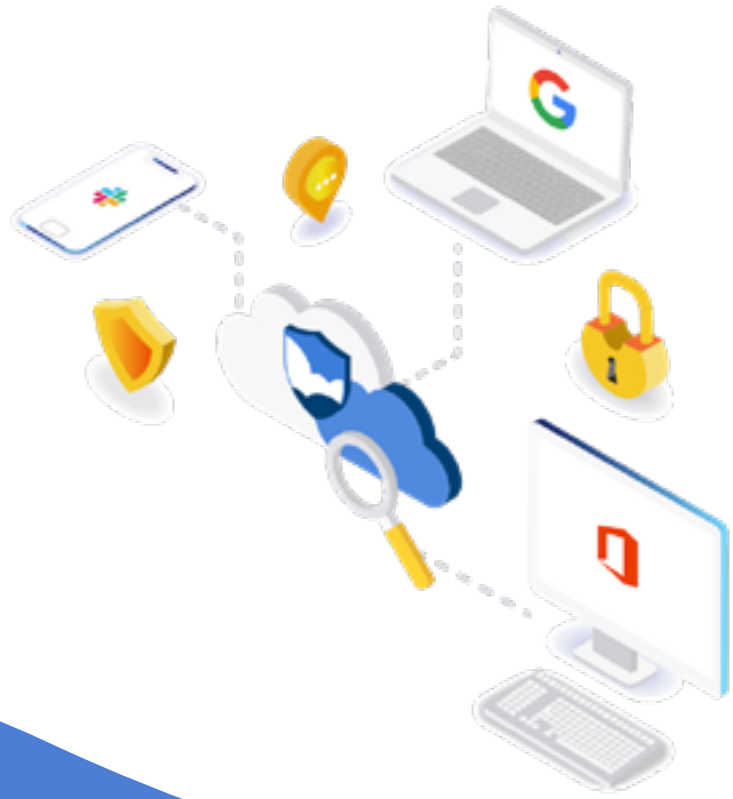
managedmethods.com | info@managedmethods.com | 303.415.3640

What Is Cloud Application Security?

Cloud application security is a series of defined policies, processes, controls, and technology governing all information exchanges that happen in collaborative cloud SaaS applications like Microsoft 365, Google Workspace, Slack, Box, etc.

As your school district moves more information and activity to the cloud, your perimeter security safeguards 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 security model.

This checklist helps you lay the groundwork for zero trust security in your school district's Google Workspace and/or Microsoft 365 apps



managedmethods.com | info@managedmethods.com | 303.415.3640

Set 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.

At minimum, you should 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 Microsoft 365

Configure Password Settings in Google Workspace

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.

Configure MFA Settings in Microsoft 365

Configure 2SV Settings in Google Workspace

Manage SaaS Access & Permissions

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 SaaS use in the classroom makes it difficult to stay on top of what apps have access to your cloud environment, what permissions are granted to them, 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 cloud accounts. This can be as simple as restricting access to risky apps, or as detailed as creating sanctioned and unsanctioned apps lists.

Configure SaaS Settings in Microsoft 365

Configure SaaS Settings in Google Workspace

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 cloud email provider's anti-phishing capabilities, and then layering additional safeguards and monitors on top of it if/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 Microsoft 365

Configure Anti-Phishing Settings in Google Workspace

Turn On Unintended External Reply Warning

One of the ways you can ensure that sensitive, internal information isn't improperly 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 Microsoft 365

Configure Unintended External Reply Settings in Google Workspace

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.

Configure External Sharing Settings in Microsoft 365

Configure External Calendar Sharing Settings

Configure External Sharing Settings in Google Workspace

Configure External Calendar Sharing Settings

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 (or, in Google's case, "Confidential Mode" which works a little differently) options.

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 Encryption Settings in Microsoft 365

Configure Confidential Mode Settings in Google Workspace

Set Up Data Loss Prevention (DLP) Policies

Fundamentally, data loss prevention is a strategy for ensuring that your district's sensitive and protected information does not inadvertently leave the company network—whether it's accidental or malicious.

System admins have the ability to set up data loss prevention (DLP) policies in both Google and Microsoft for Education editions. These policies help you maintain and 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 an employee 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 and/or quarantine the file.

Configure DLP Settings in Microsoft 365

Configure DLP Settings in Google Workspace

Enable Mobile Management

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

Configure Mobile Management Settings in Microsoft 365

Configure Mobile Management Settings in Google Workspace

Run A Security Health Audit

Once you've completed this checklist, it's a good idea to run a security audit of your Google and/or Microsoft 365 environment. An audit will re-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 the security health of your cloud applications.

Configure Security Audits in Microsoft 365

Configure Security Audits in Google Workspace

Managed Methods

Cloud Security Made Easy

K-12 Cybersecurity & Safety — Made Easy!

ManagedMethods makes securing your district's Google Workspace and/or Microsoft 365 data easy. The platform provides malware and phishing protection and data loss prevention for cloud-based email, files, and shared drive applications. ManagedMethods uses advanced machine learning technology to detect account takeovers, a growing issue in cloud security.

Using ManagedMethods, system admins can quickly and easily determine where security risks exist, remediate security issues, and set up customizable data loss prevention policies.

Experience How ManagedMethods Provides Easy Visibility and Control

Demo On-Demand
Click Here To Watch

managedmethods.com | info@managedmethods.com | 303.415.3640