NETWORK MAINTENANCE AND SECURITY

for Schools and Districts

Each year, network administrators and district leaders must take time to review their current network infrastructure, especially their cybersecurity solutions, and conduct any maintenance, replacements, or patches that have been waiting to be addressed.

MONTHLY CHECKLIST

When it comes to network maintenance, creating a standard checklist for school-year maintenance can ease the in-depth audit conducted during summer months. During the school year, network administrators should:

ROUTINELY BACKUP ALL DATA

Setting automated backups for all critical data will ensure that if anything is compromised on the network, information can be readily available. These backups should also be kept off the network as an additional security measure.

VERIFY NETWORK UTILIZATION

As more devices are connected to the network, servers are at risk of running out of capacity. Routinely monitoring devices and applications and keeping track of data usage can highlight any bandwidth issues before they become crippling.

KEEP SOFTWARE PLUGINS AND PATCHES UP-TO-DATE

As software updates and plugins become available they should be implemented in the current system. These patches and plugins usually address security vulnerabilities and come from the manufacturer.

CHANGE PASSWORDS REGULARLY

Setting a routine cadence for password updates is a critical component of good cyber hygiene and protecting the network against anyone who gains unauthorized access.

ANNUAL AUDIT

During the summer months, when there is less overall traffic on the network, a deeper audit and inspection of the network can occur. Many times, this is also an ideal setting to test and compare alternative vendors for both hardware and software solutions that may be more aligned with district goals. This Summer Audit should include the following:

DIRECTORY ACCESS CLEAN UP

Network administrators should conduct a Directory Access Audit, disabling access to data of students who no longer attend the school, removing access for staff or contractors who also no longer work with the school, and ensure that those who still have access are grouped according to policy and information privilege.

HARDWARE TESTS

For school districts with on premises data centers, checking event logs for overheating notices, network failures, or other errors can be an early sign of a potential hardware failure. Analyze how often any or all of these incidents occurred to understand frequency and if the system is working within its normal range.

UPDATE LICENSING AGREEMENTS

Performing an assessment about software and application in use, duration of current licensing agreement, the projected usage for the incoming school year and help IT teams better manage funding, inventory, and keep diligent records for each agreement.

FIREWALL CHECK

During these months, conducting a stringent review of the current firewall software is essential. This Firewall check should include a review of blocked or flagged items, and deciding whether or not to add additional security items to the list, VPN settings, rules allowing public web traffic, and web filtering policies and search criteria.

COMPLIANCE REVIEW

Each year new regulations are introduced to keep students safe while also protecting their privacy and data. Regulations such as CIPA, the Family Education Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), and **K-12 Cybersecurity Act of 2019** remain the cornerstone for K-12 schools. It is important to make sure that any additional network changes meet these requirements and if new regulations go into effect, that the current network is up to par.

Technology will continue to transform how teachers and administrators connect to their students in the classroom and at home. Establishing a routine maintenance checklist and comprehensive audit for IT departments will support these technology adoptions while protecting the network from cybercriminals.

HOW CAN UNTANGLE HELP?

Customers choose Untangle for next generation web filtering which includes application control, SSL inspection and bandwidth management, along with the ability to block, flag and alert on search terms, enforce safe search, and log YouTube searches, breaking down the glass wall of how students and teachers can safely access educational materials from across the internet.

PROTECT

Untangle's Web Filter helps cybersecurity teams get a handle on rogue applications and malicious content that causes harm when accessed from web pages. Advanced web filtering technology also deploys "safe search" parameters, blocking harmful content on the most common search engines, such as Google, Yahoo, and Bing.

FILTER

Untangle's Web Filter helps cybersecurity teams get a handle on rogue applications and malicious content that causes harm when accessed from web pages. Advanced web filtering technology also deploys "safe search" parameters, blocking harmful content on the most common search engines, such as Google, Yahoo, and Bing. In addition, KidzSearch filtering ensures that all results are filtered through an additional layer for age-appropriate content.

CONNECT

Untangle's OpenVPN and Tunnel VPN solutions help cybersecurity teams keep users and data safe, no matter their location or level of access.

Administrative teams can create private and secure connections for remote students, teachers, and other district employees, and thus maintain visibility and control over remote workers.

MANAGE

Untangle's Policy Manager lets administrators define network privileges based on username, group, device, time, protocol, and more to control who can access websites, data, or apps. In addition, the Reports app provides teams with detailed views of network traffic, and Command Center enables staff to manage network traffic across multiple locations.

BACKUP

Schools and districts can utilize NG Firewall's Configuration Backup tool to ensure uninterrupted protection, availability, and business continuity. Recover easily from unavoidable hardware failures and unforeseen disasters by safeguarding policies and other settings in the cloud, via either Untangle's Command Center or Google Drive.