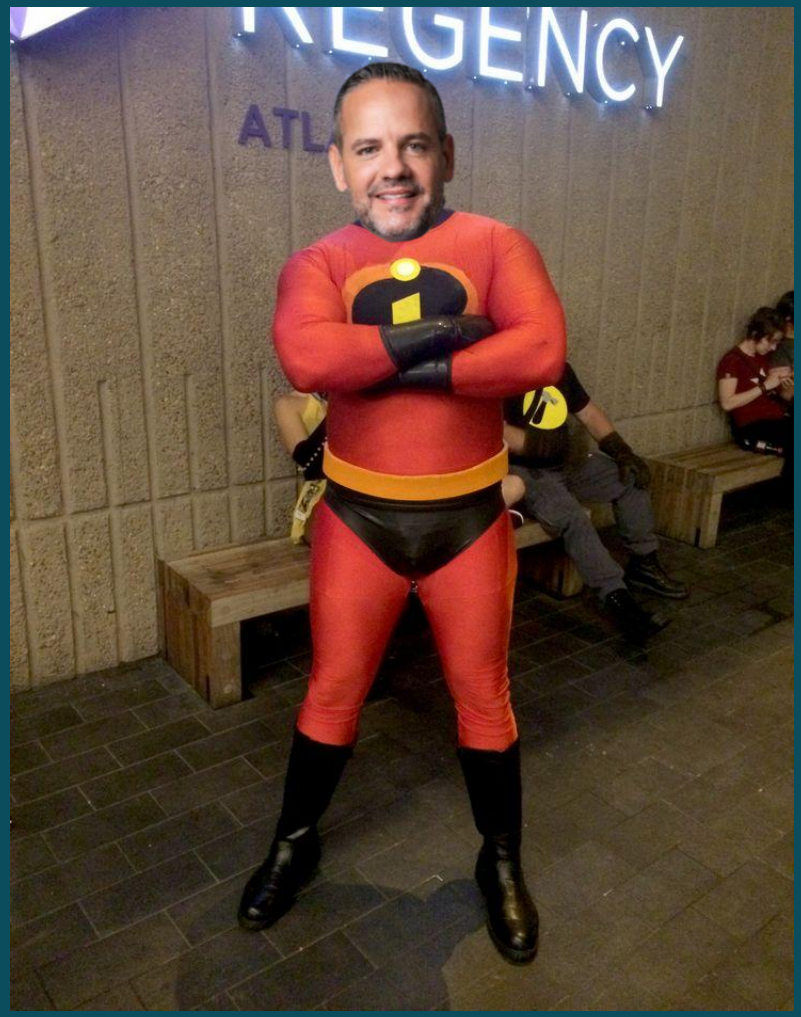
IT for Education

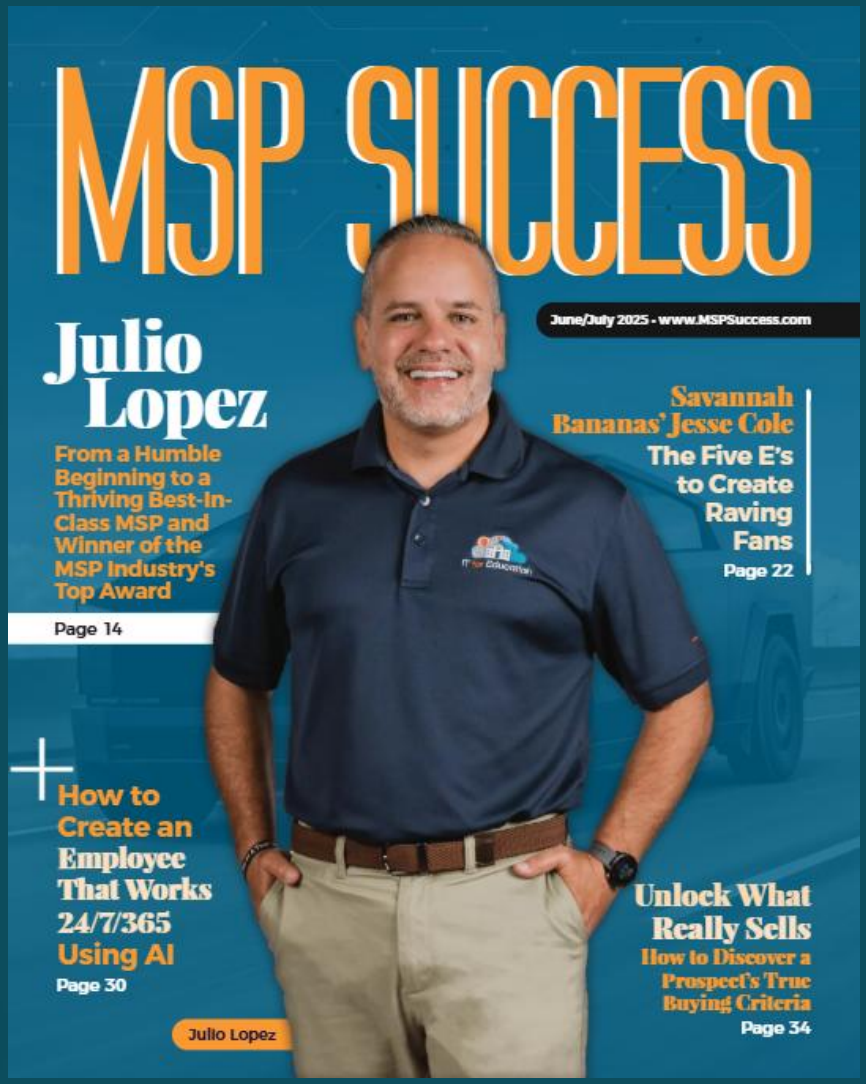
CYBERSECURITY

What Every Administrator Needs to Know

Navigating the Archdiocese of Miami's Minimum Security Standards


THINKER
ThinKing Cap
IDEAOMETER


REGENCY

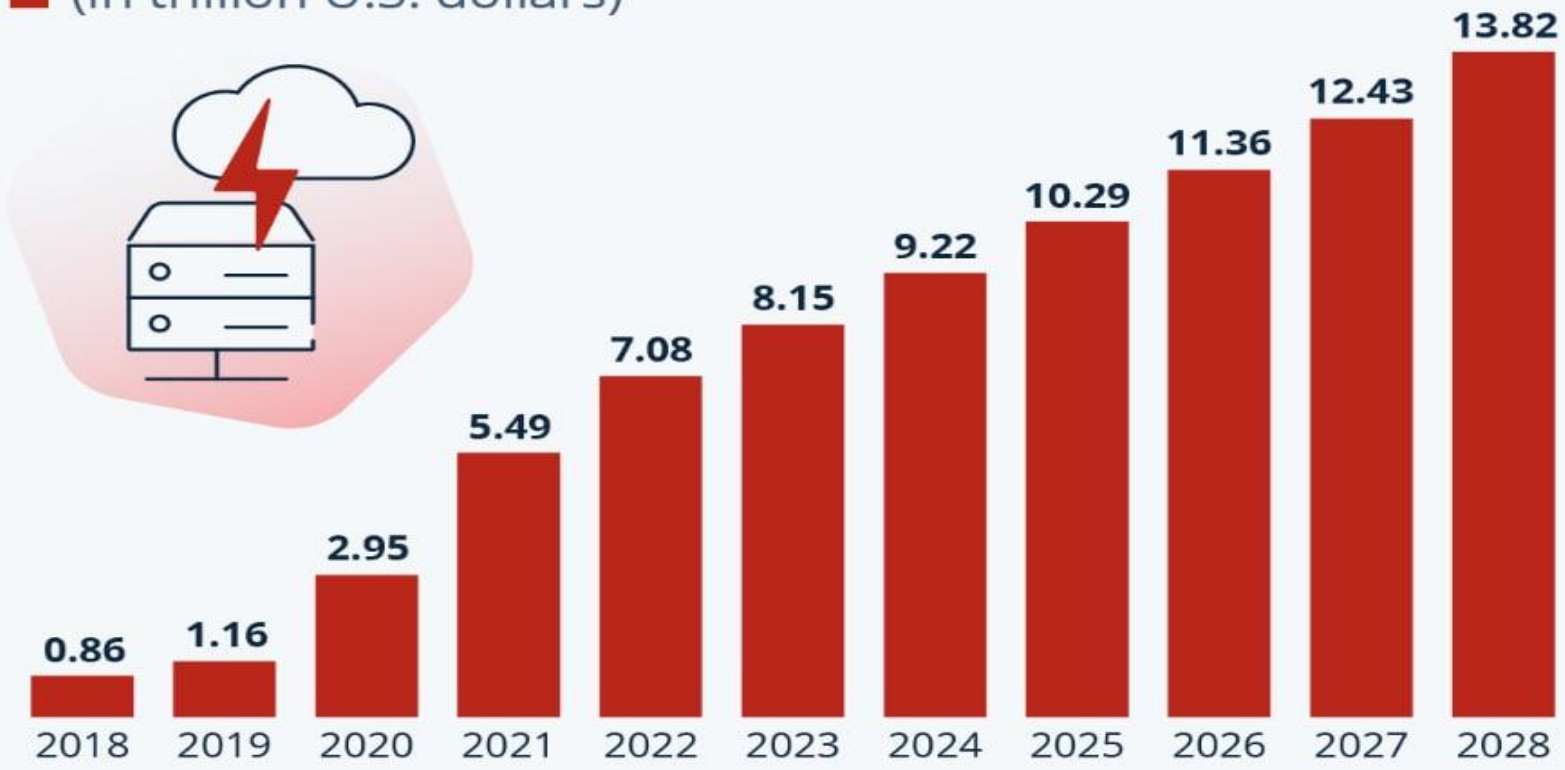

MSP SUCCESS
June/July 2025 - www.MSPSuccess.com
Julio Lopez
From a Humble Beginning to a Thriving Best-In-Class MSP and Winner of the MSP Industry's Top Award
Page 14
Savannah Bananas' Jesse Cole
The Five E's to Create Raving Fans
Page 22
How to Create an Employee That Works 24/7/365 Using AI
Page 30
Unlock What Really Sells
How to Discover a Prospect's True Buying Criteria
Page 34
Julio Lopez

Why am I here today?


GROUND
RULES

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

St. Thomas the Apostle
Catholic School

recognized as
Blue Ribbon School of Excellence


JACK
OF ALL
TRADES
Happy Hal
PROPRIETOR

Something has to change...

Good news!

ADOM Minimum Security Standards (MSS) Compliance Checklist

Deadline: All guidelines must be implemented by December 31, 2025.

Use this checklist to verify your school's compliance. If you cannot confidently check every box, schedule a discovery call with us to ensure you're protected.

Core Security

1. All devices are running **supported operating systems** with the latest security patches.
2. All devices have **anti-malware/antivirus software** enabled (e.g., Windows Defender, Malwarebytes).
3. **Host-based firewalls** are enabled on computers, printers, and networked equipment.
4. A **network-based firewall** is active and configured to block unauthorized inbound traffic.
5. Web-filtering system to comply with CIPA guidelines.

Networks & Wireless

1. Wi-Fi uses **WPA2 at minimum.**
2. Wireless controllers and access points require **complex passwords**.
3. **SSH** (not Telnet) is used for CLI management of network devices.
4. Guest Wi-Fi is **segmented** and separate from internal/production networks.

Passwords & Authentication

1. All passwords meet **complexity requirements** (refer to ADOM MSS Guidelines).
2. Default/blank passwords have been **changed or disabled**.
3. PINs on mobile devices are at least **6 digits**.
4. **Passwords are unique** per account and not reused across systems.
5. **2FA/MFA is enabled** for email and remote access.
6. Biometric authentication is enabled where supported.

Devices

1. Devices automatically **lock after 15 minutes** (5 minutes for mobile).
2. Laptops are encrypted (e.g., BitLocker, File Vault).
3. Mobile devices are **not jailbroken/rooted** and only connect to **guest Wi-Fi**.

Remote Access & Accounts

1. Remote desktop and terminal access are **restricted** through secure VPN/proxy.
2. Remote access tools (TeamViewer, AnyDesk, etc.) use **MFA** and rotate passwords every 30 days.
3. Administrator accounts are **separate from user accounts** and not used for daily tasks.
4. Built-in local admin accounts are **disabled or renamed** with strong credentials.

Data Protection

1. Backups are performed **daily** with version history.
2. Backups are **tested, encrypted, and stored offline/offsite**.
3. Old/unused data is archived and removed from production systems.
4. Protected data (SSNs, credit cards, etc.) is stored securely with **AES encryption**.

Servers, Networks & Virtual Environments

1. Servers use complex passwords, remove unnecessary ports/services, and auto-lock.
2. Virtual environments (VMs, iSCSI, vMotion) are **network-segmented**.
3. All network authentication and traffic use **secure, encrypted protocols** (HTTPS, SSH, etc.).

Email & Web

1. Users are trained to identify **phishing/scam emails** at minimum.
2. All external emails are labeled with a **warning disclaimer**.
3. Browsers are updated and **do not store passwords**.

Documentation

1. An **inventory of software and data types** is maintained.
2. All changes to network, servers, or software are **documented**.
3. End-of-life hardware/software has been **upgraded or discarded**.

If you left any of these items unchecked or are unsure, your school may not be MSS compliant.

Book a **free discovery call** today to verify compliance before the **December 31, 2025,** deadline.

Cybersecurity Threats In Schools

Featuring:

Adonis Sardiñas

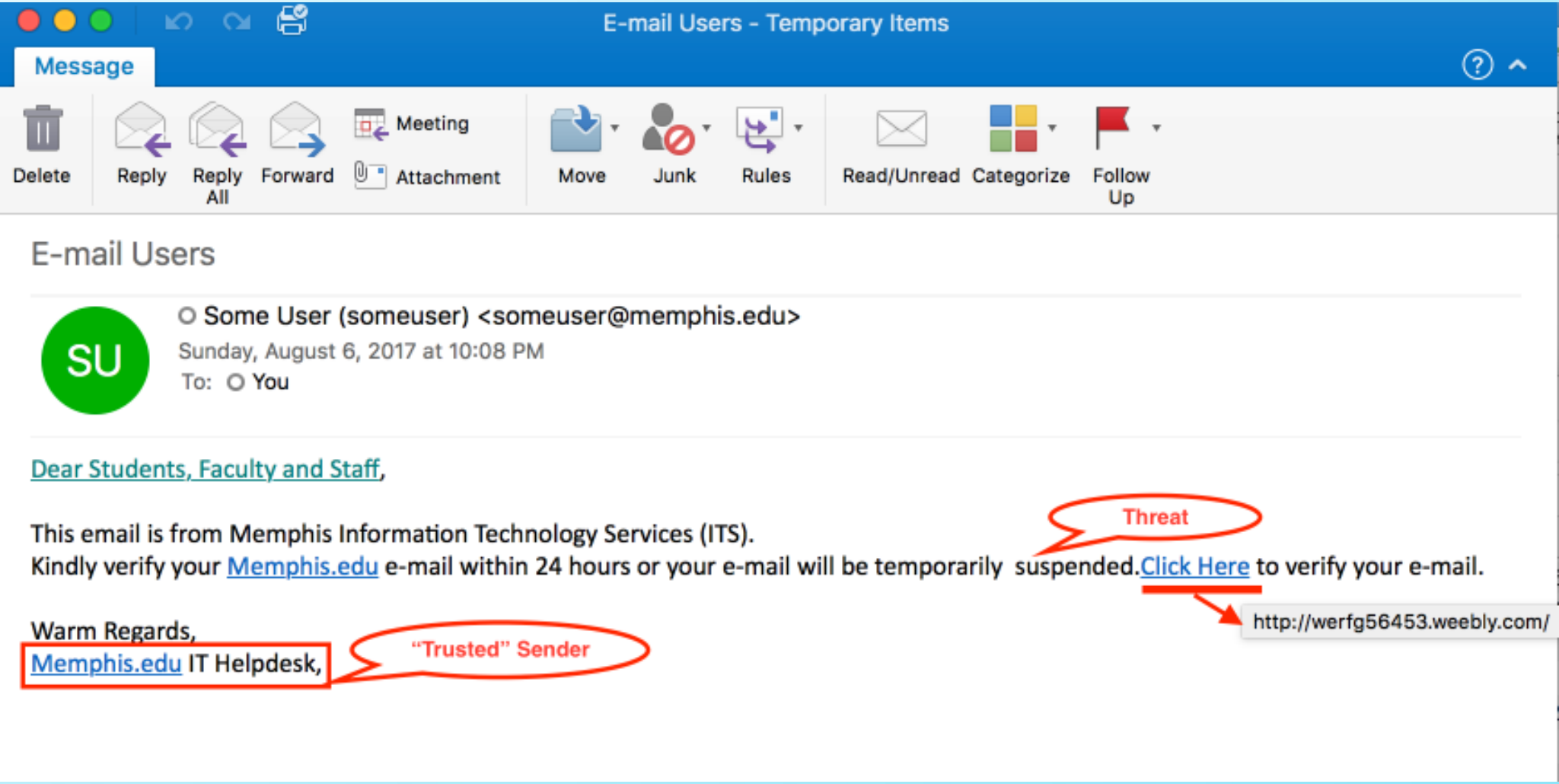
Cyber Engineer – Fortinet

Cybersecurity professor – FIU

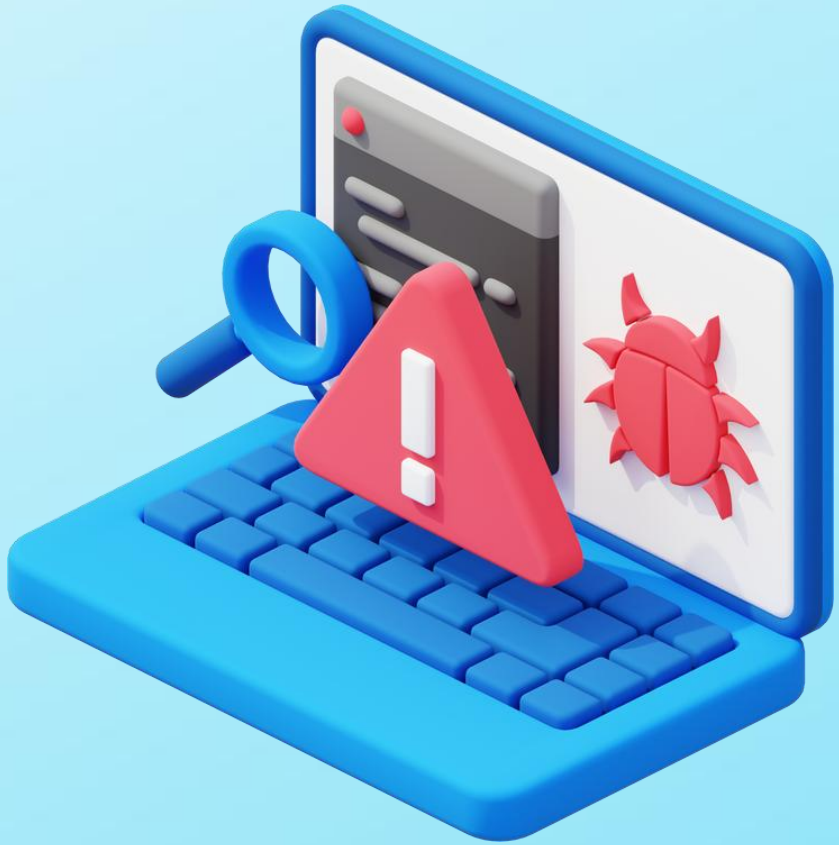
Phishing & Social Engineering Attacks

Example Scenario:

An email that looks like it’s from the principal asking teachers to “reset their password.


E-mail Users - Temporary Items
Message
Delete
Reply
Reply All
Forward
Meeting
Attachment
Move
Junk
Rules
Read/Unread
Categorize
Follow Up
E-mail Users
SU
Some User (someuser) <someuser@memphis.edu>
Sunday, August 6, 2017 at 10:08 PM
To: You
Dear Students, Faculty and Staff,
This email is from Memphis Information Technology Services (ITS).
Kindly verify your Memphis.edu e-mail within 24 hours or your e-mail will be temporarily suspended.Click Here to verify your e-mail.
Threat
http://werfg56453.weebly.com/
Warm Regards,
Memphis.edu IT Helpdesk,
"Trusted" Sender

Ransomware & Data Breaches



Example Scenario:

In 2021, Broward County Public Schools, one of the largest districts in Florida, was hit by a massive ransomware attack. Hackers demanded $40 million and stole personal data, including Social Security numbers and health information, from about 50,000 students and staff. The district refused to pay, but the breach caused major disruptions and damaged trust in the school system.

Insecure Devices & Networks

Example Scenario:

A hacked printer or camera could give attackers a way into the entire network.

Compliance & Data Privacy

- **FERPA:** Protects student education records.
- **COPPA:** Safeguards online data of children under 13.
- **CIPA:** Requires schools to filter harmful content and monitor student internet use.

- **NIST CSF (Cybersecurity Framework):** Provides a structured approach to managing risk across five areas: Identify, Protect, Detect, Respond, and Recover.
- **CIS Controls:** A prioritized set of best practices to defend against the most common cyber threats, often used as a practical roadmap for schools with limited resources.

Non-Compliance can lead to:

- Legal penalties and loss of funding.
- Loss of trust among parents, students, and the community.
- Increased vulnerability to attacks and misuse of sensitive student information.

Cybersecurity Best Practices

Featuring:

Adonis Sardiñas

Cyber Engineer – Fortinet

Cybersecurity professor – FIU

Strong Passwords & Multi-Factor Authentication (MFA)

Example Scenario:

A staff member’s email password is stolen. Without MFA, attackers can reset grades or spread phishing emails across the district. With MFA, the stolen password alone is useless.

Cybersecurity Awareness Training

Example Scenario:

Without proper awareness, a teacher might leave a laptop unlocked in a classroom or a student might download a suspicious app onto a school device. Either scenario could allow unauthorized access to sensitive data or spread malware across the network.

Regular Software Updates & Patch Management

Example Scenario:

An unpatched school server running outdated Windows was exploited to spread ransomware across the entire network.

Data Backup & Recovery Plans

Example Scenario:

Imagine a school’s main server crashes during finals week, wiping out grade records and lesson plans. With tested backups in place, the data can be quickly restored, avoiding chaos. Without them, the school could face days or weeks of disruption.

Secure Networks & Devices

Example Scenario:

A hacker accessed a school network by exploiting an unsecured Wi-Fi guest account, then jumped into student records. Segmentation would have stopped the lateral movement.

MSS Compliance Checklist

IT for Education

+

ADOM Minimum Security Standards (MSS) Compliance Checklist

Deadline: All guidelines must be implemented by December 31, 2025.

Use this checklist to verify your school's compliance. If you cannot confidently check every box, schedule a discovery call with us to ensure you're protected.

Core Security

1. All devices are running **supported operating systems** with the latest security patches.
2. All devices have **anti-malware/antivirus software** enabled (e.g., Windows Defender, Malwarebytes).
3. **Host-based firewalls** are enabled on computers, printers, and networked equipment.
4. A **network-based firewall** is active and configured to block unauthorized inbound traffic.
5. Web-filtering system to comply with CIPA guidelines.

Networks & Wireless

1. Wi-Fi uses **WPA2 at minimum.**
2. Wireless controllers and access points require **complex passwords**.
3. **SSH** (not Telnet) is used for CLI management of network devices.
4. Guest Wi-Fi is **segmented** and separate from internal/production networks.

Passwords & Authentication

1. All passwords meet **complexity requirements** (refer to ADOM MSS Guidelines).
2. Default/blank passwords have been **changed or disabled**.
3. PINs on mobile devices are at least **6 digits**.
4. **Passwords are unique** per account and not reused across systems.
5. **2FA/MFA is enabled** for email and remote access.
6. Biometric authentication is enabled where supported.

Devices

1. Devices automatically **lock after 15 minutes** (5 minutes for mobile).
2. Laptops are encrypted (e.g., BitLocker, File Vault).
3. Mobile devices are **not jailbroken/rooted** and only connect to **guest Wi-Fi**.

Remote Access & Accounts

1. Remote desktop and terminal access are **restricted** through secure VPN/proxy.
2. Remote access tools (TeamViewer, AnyDesk, etc.) use **MFA** and rotate passwords every 30 days.
3. Administrator accounts are **separate from user accounts** and not used for daily tasks.
4. Built-in local admin accounts are **disabled or renamed** with strong credentials.

Data Protection

1. Backups are performed **daily** with version history.
2. Backups are **tested, encrypted, and stored offline/offsite**.
3. Old/unused data is archived and removed from production systems.
4. Protected data (SSNs, credit cards, etc.) is stored securely with **AES encryption**.

Servers, Networks & Virtual Environments

1. Servers use complex passwords, remove unnecessary ports/services, and auto-lock.
2. Virtual environments (VMs, iSCSI, vMotion) are **network-segmented**.
3. All network authentication and traffic use **secure, encrypted protocols** (HTTPS, SSH, etc.).

Email & Web

1. Users are trained to identify **phishing/scam emails** at minimum.
2. All external emails are labeled with a **warning disclaimer**.
3. Browsers are updated and **do not store passwords**.

Documentation

1. An **inventory of software and data types** is maintained.
2. All changes to network, servers, or software are **documented**.
3. End-of-life hardware/software has been **upgraded or discarded**.

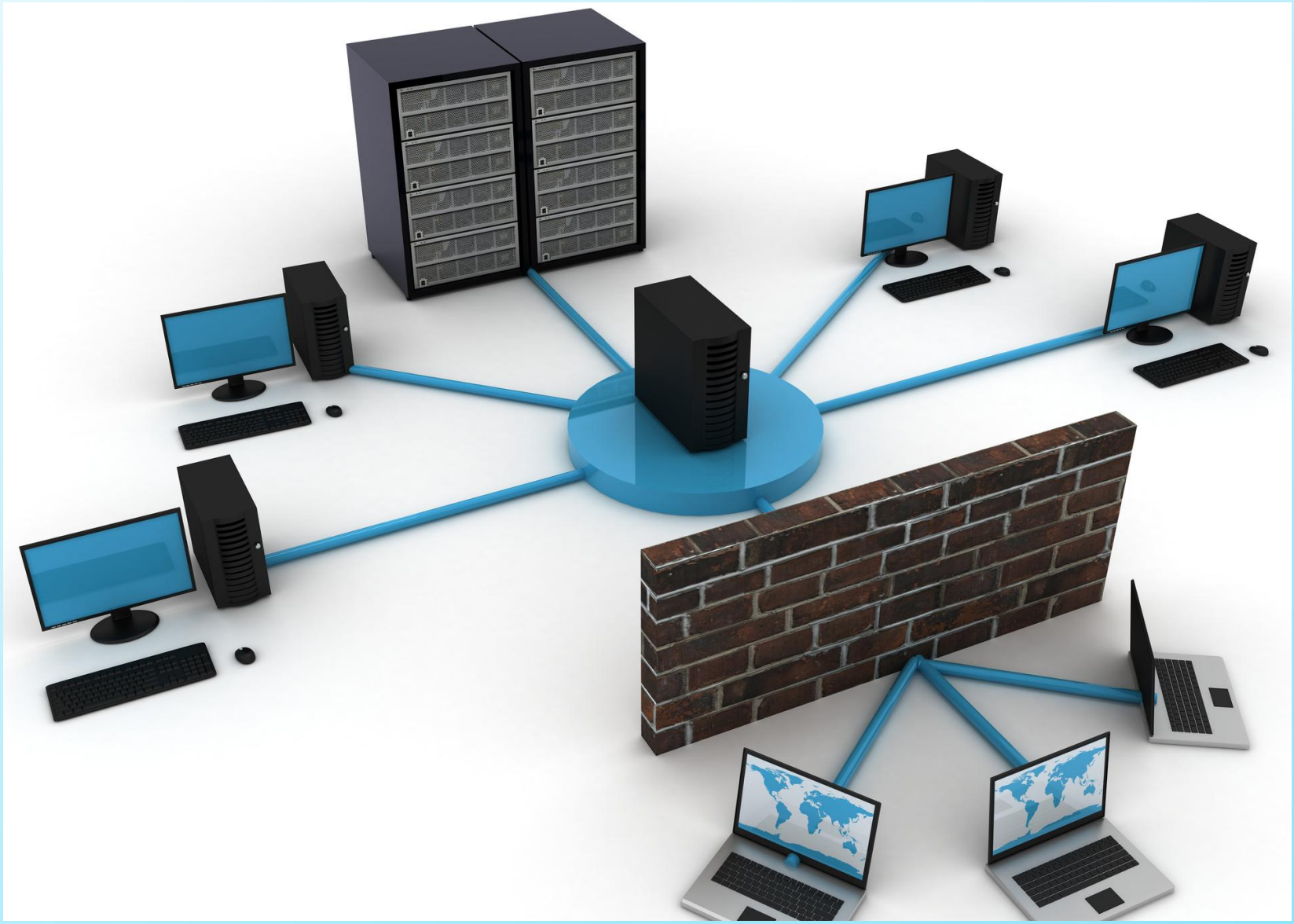
If you left any of these items unchecked or are unsure, your school may not be MSS compliant.

Book a **free discovery call** today to verify compliance before the **December 31, 2025,** deadline.

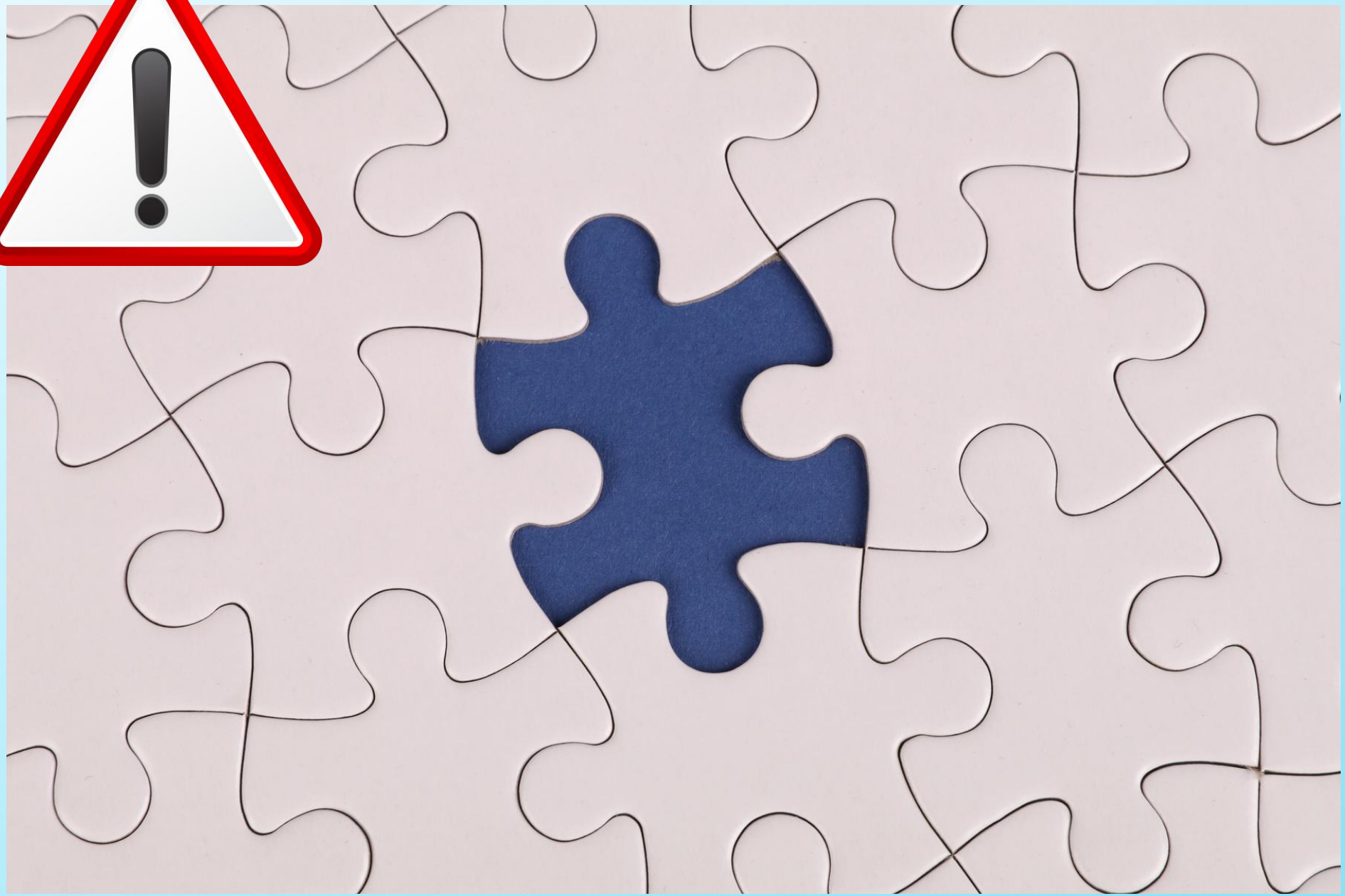
Core Security

Refer to section II.A in ADOM MSS Guidelines for more details.

Refer to section II.B in ADOM MSS Guidelines for more details.



Refer to sections II.C-D in ADOM MSS Guidelines for more details.



Networks & Wireless

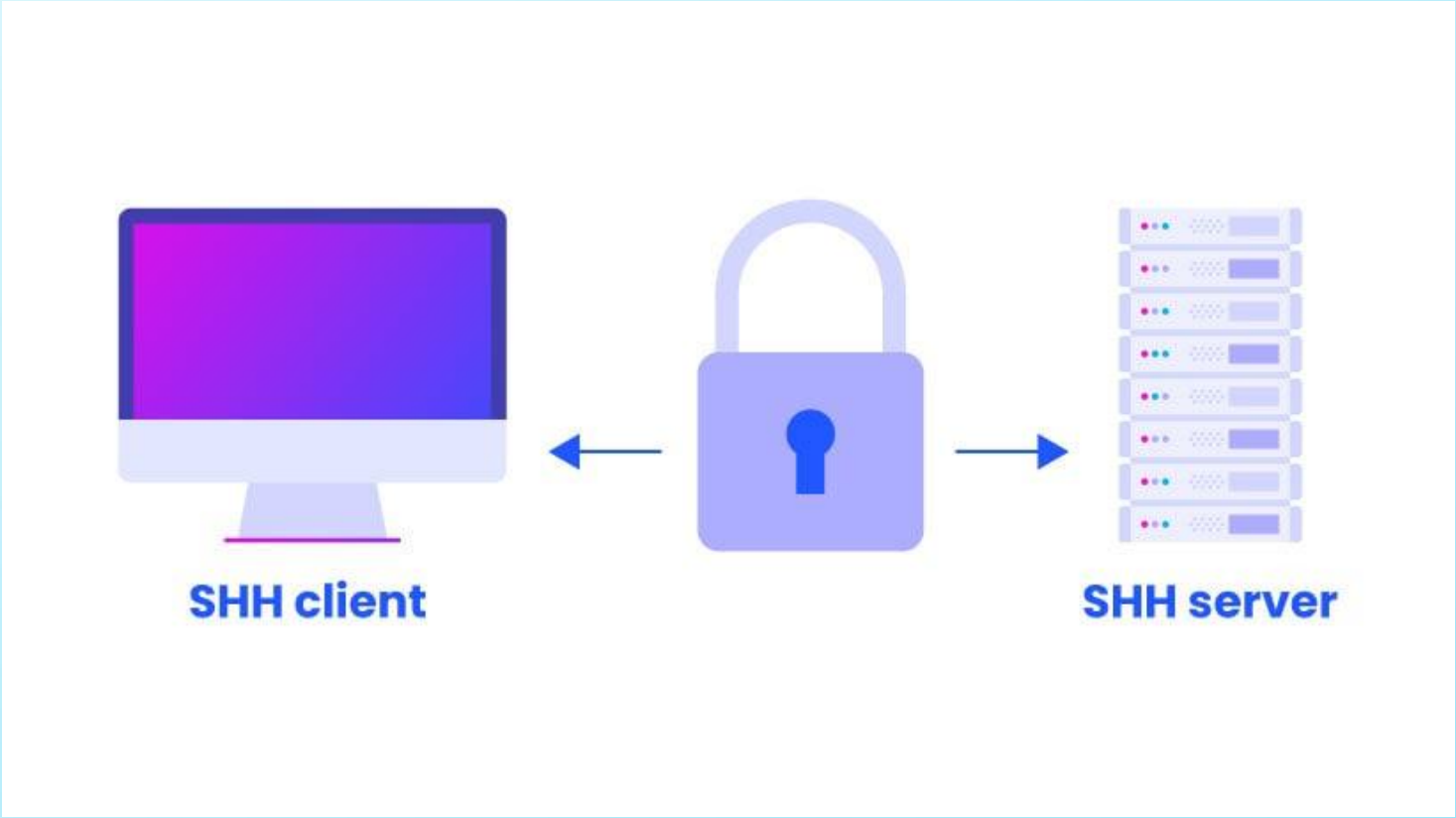
Wi-Fi must be WPA2 at minimum.

Refer to section II.E in ADOM MSS Guidelines for more details.

Your wireless controllers and access points must have strong passwords.

Refer to section II.F in ADOM MSS Guidelines for more details.

SSH > Telnet



Refer to section II.P in ADOM MSS Guidelines for more details.

Strong passwords.

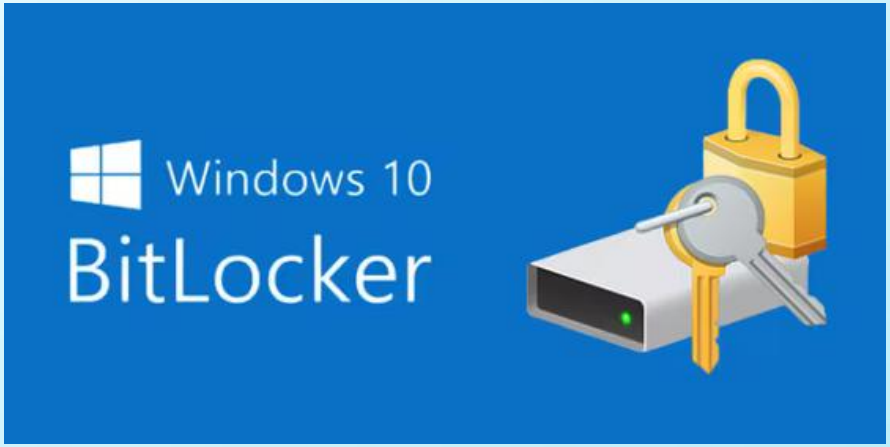
Two-factor MFA.

15-minute automatic device lock.

At least a 6-digit PIN for mobile devices.

Refer to sections II.F-G and II.M-N in ADOM MSS Guidelines for more details.

Device encryption



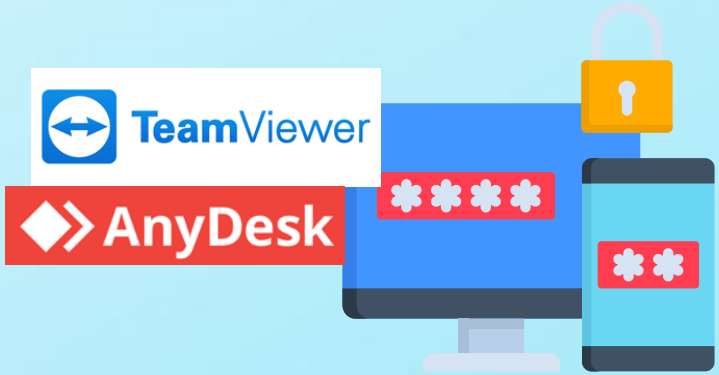
No jailbreaking

Guest Wi-Fi only

Refer to sections II.H and II.P in ADOM MSS Guidelines for more details.

Remote access requires a VPN or proxy

MFA + passwords



Separate from user accounts

Disable/rename local accounts.

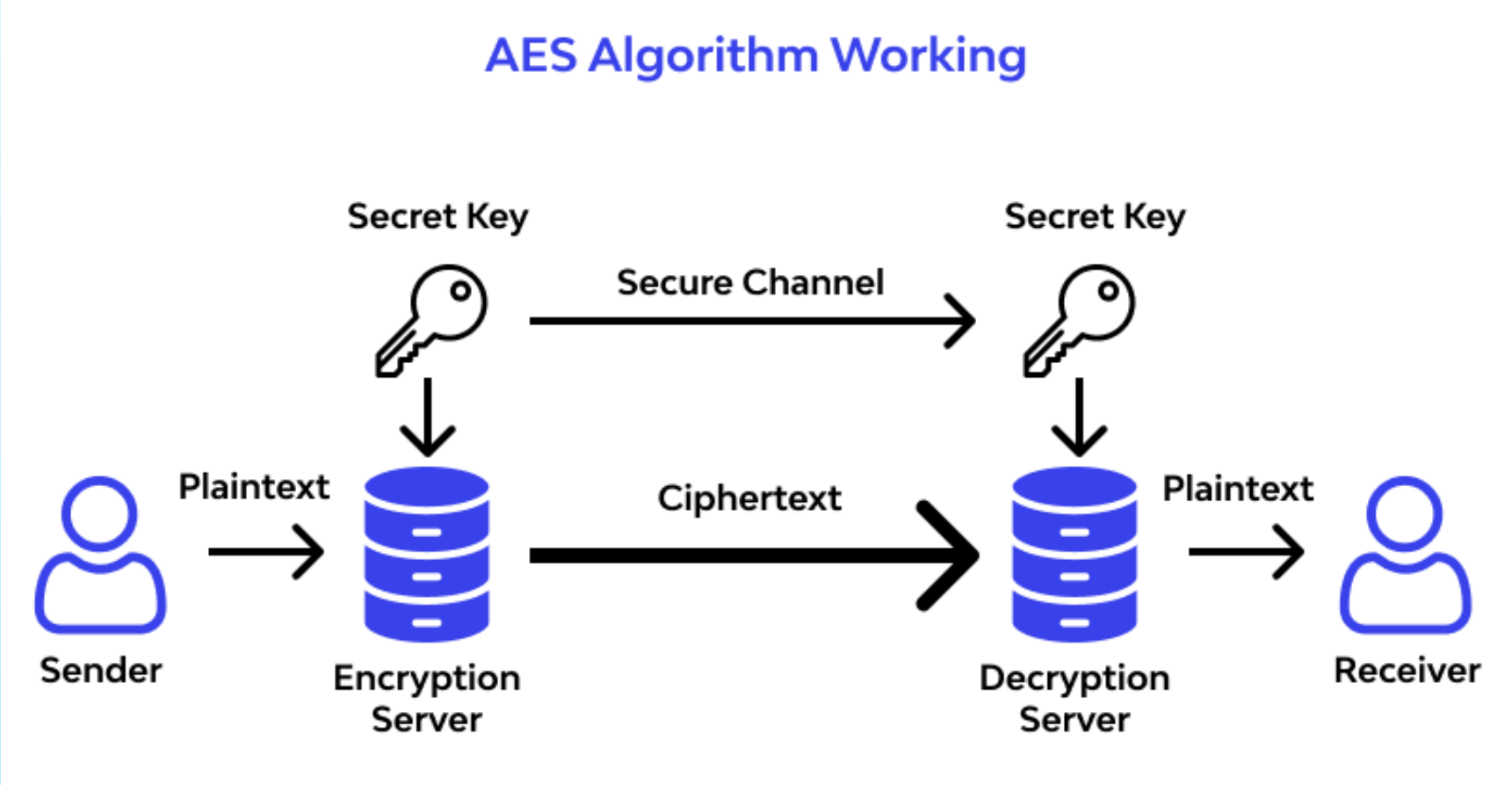
Refer to section II.H-J in ADOM MSS Guidelines for more details.

Daily backups

Archive old data

Refer to sections II.K-L in ADOM MSS Guidelines for more details.

AES Standards for encryption

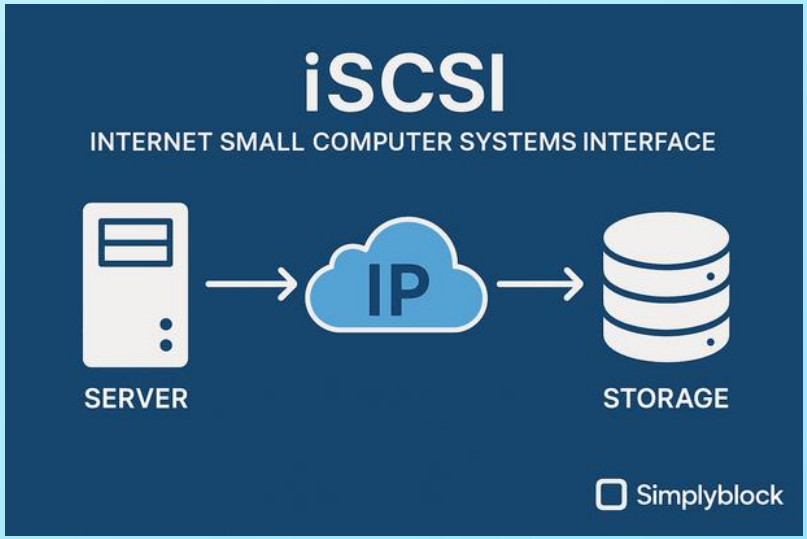


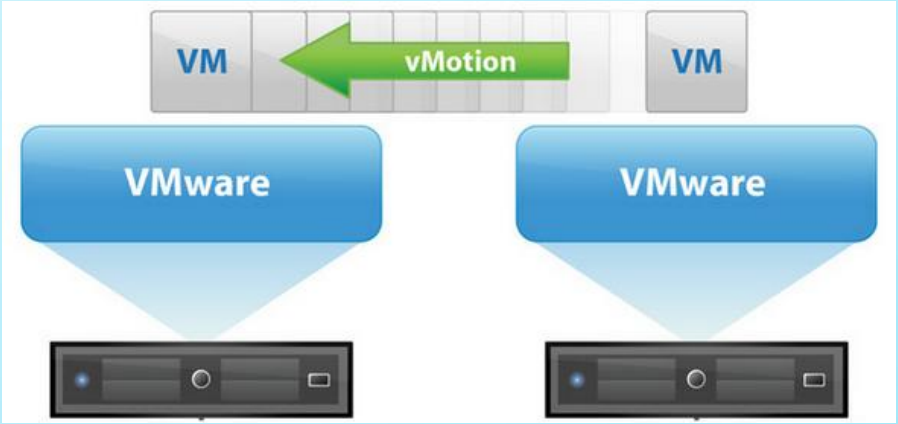
Refer to sections II.K-L in ADOM MSS Guidelines for more details.

Servers + Virtual Environments

Refer to sections II.Q-R in ADOM MSS Guidelines for more details.

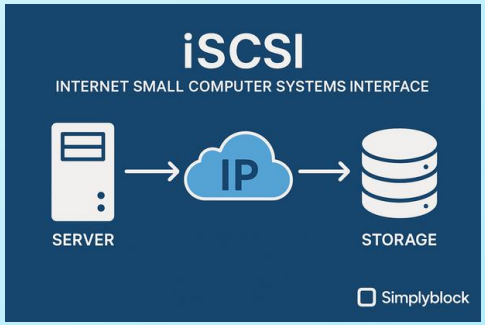
Virtual Environments

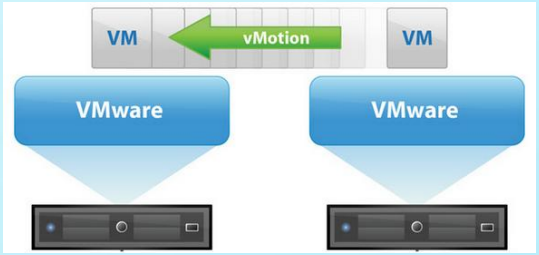




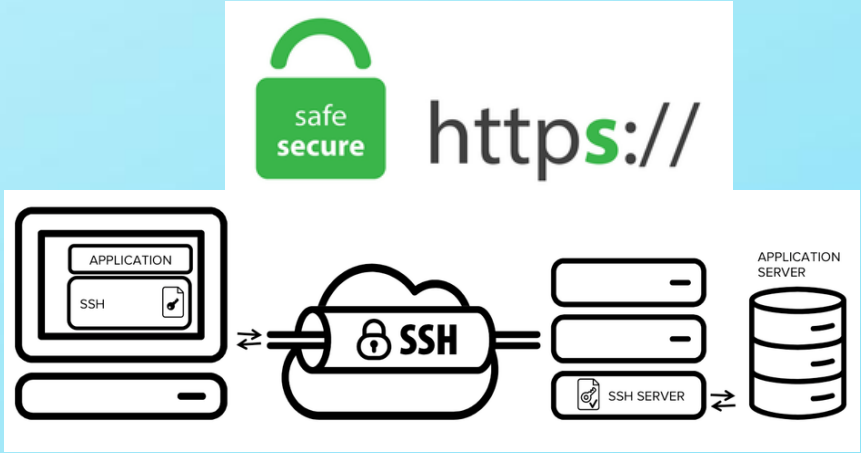
Refer to sections II.Q-R in ADOM MSS Guidelines for more details.

Virtual Environments





Encryption



Refer to sections II.Q-R in ADOM MSS Guidelines for more details.

Email and Web

Refer to sections II.S-T in ADOM MSS Guidelines for more details.

Email and Web

Refer to sections II.S-T in ADOM MSS Guidelines for more details.

Email and Web

Refer to sections II.S-T in ADOM MSS Guidelines for more details.

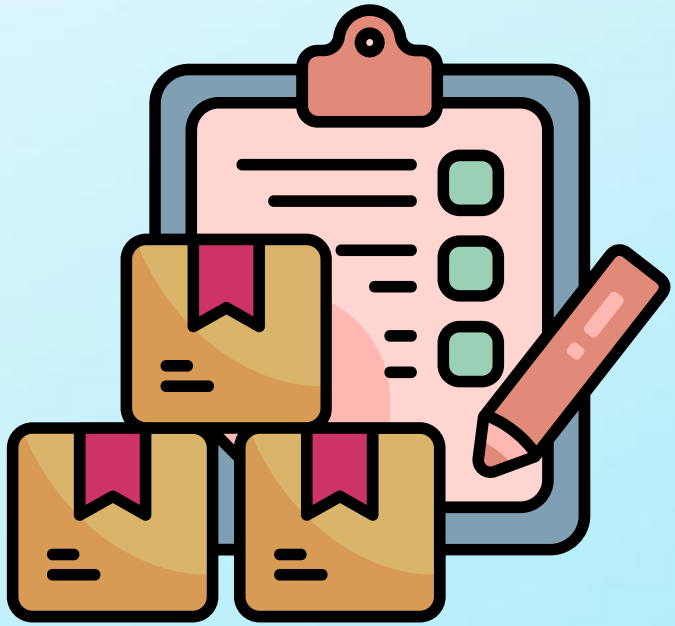
Email and Web

Refer to sections II.S-T in ADOM MSS Guidelines for more details.

Email and Web

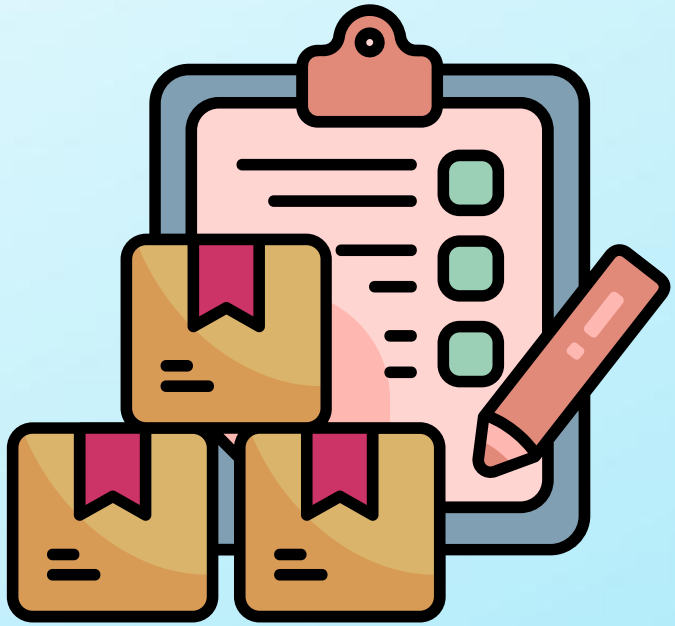
Refer to sections II.S-T in ADOM MSS Guidelines for more details.

Documentation



Refer to sections II.U-V in ADOM MSS Guidelines for more details.

Documentation



End-of-life
software/hardware

Refer to sections II.U-V in ADOM MSS Guidelines for more details.

Thank you!

(305) 403-7582
www.itforedu.com/schedule
ask@itforedu.com

Register for our free
E-Rate webinar

www.itforedu.com/e-rate-webinar/