NTS201

Ashley Kennedy

University of Advancing Technology

Final Project: Security Plan

Professor Rodriguez

August 24, 2025

Table of Contents

SECURITY PLAN

A&E Total Transformations

Date: August 15, 2025

Policy Number: AE-001

Last Updated: August 15, 2025

Next Review Date: January 9, 2026

1. Objectives and Scope

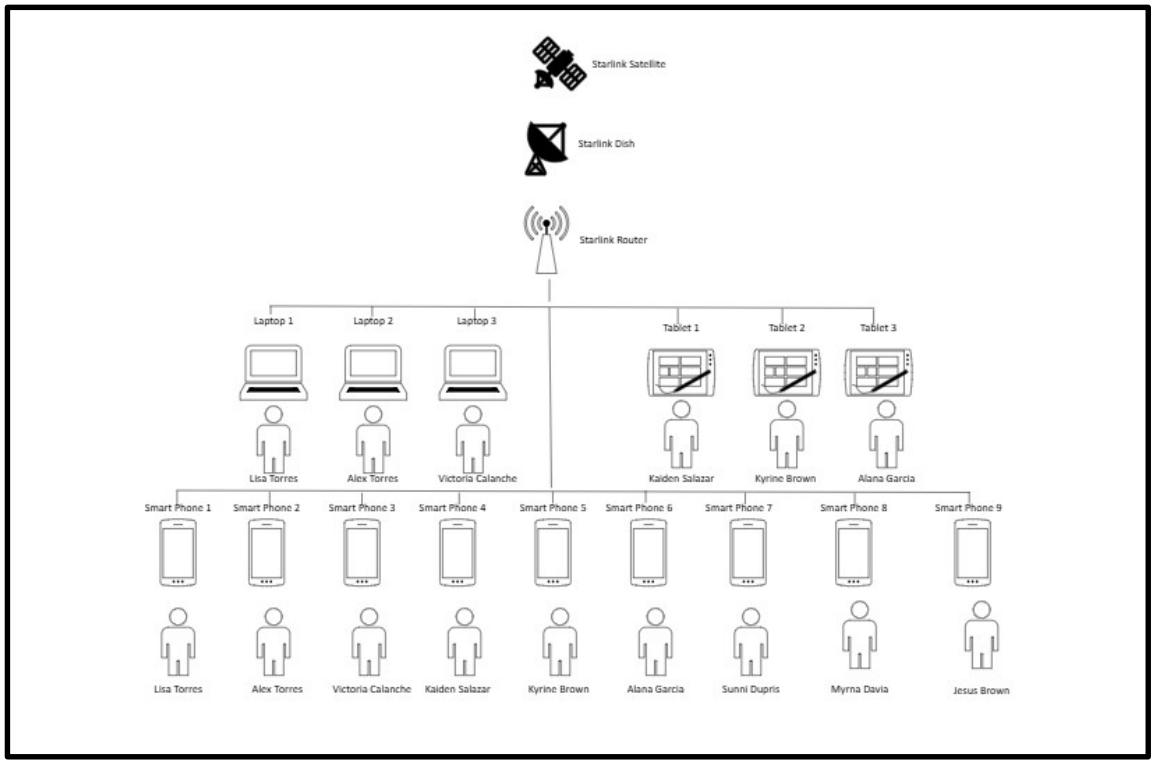
A&E Total Transformations' primary goal is to safeguard all company assets to include computer hardware/software and other physical equipment as well as staff/users against unauthorized access, disclosure, alteration, and destruction. This plan is applicable to all systems and networks within the company's infrastructure.

2. Network Architecture

Current Employees: 9

Name	Privilege Level	Full access to all system settings and sensitive data to ensure network and systems work properly
Lisa Torres	High	Yes
Alex Torres	High	Yes
Victoria Calanche	Medium	No
Kaiden Salazar	Low	No
Kyrine Brown	Low	No
Alana Garcia	Low	No
Sunni Dupris	Low	No
Myrna Davis	Low	No
Jesus Brown	Low	No

Network Infrastructure:



Background: A&E Total Transformations is a small local business that specializes in home renovations and general construction. The hardware for Starlink will remain at the owner's residence. A&E Total Transformations operates primarily off our cell phones and personal devices. Starlink fits our business structure best because we are constantly on the move. Meaning, we're out in the community meeting with clients, on job sites or gathering equipment at home improvements stores. It's crucial for us to have the ability to connect to a reliable network throughout the day. We're rarely sitting at a desk and need our laptops, tablets and phones up and running for proper communication with office staff, laborers, contractors and clients.

Starlink: Starlink provides two IPv4 policies, default and public and always provides a public IPv6/56 prefix. Starlink does not provide static IP addresses. Starlink network is dynamic and from time-to-time IP addresses will change for resilience, as network capacity increases, or when new countries are added to the network. Mobile users may experience IP address changes when moving locations and states that the changes will cause a brief DHCP handoff outage. Furthermore, it states that Starlink's service has many different routers in different locations to provide the lowest latency connection possible.

Starlink's default IPv4 configuration is Carrier Grade Network address Translation (CGNAT) using private address space assigned to Starlink clients using DHCP from the 100.64.0.0/10 prefix. Network Address Translation (NAT) translates between Starlink private and public IPs. Starlink also states that public IP is reachable from any device on the internet and is assigned to Starlink network clients using DHCP. And lastly, when it comes to up allocation, Starlink will allocate:

> Public IPv4 address for the customer's wide area network (WAN), provisioned via Dynamic Host Configuration Protocol version 6 Prefix Delegation (DHCP) for routers/firewalls using IPv4.

IPv6 /64 prefix for the customer's wide area network (WAN), provisioned via Stateless Address Auto Configuration (SLAAC) for routers/firewalls using IPv6.

IPv6 /56 prefix for the customer's local area network (LAN), provisioned to routers capable of issuing a DHCPv6-PD request.

For DHCP Configuration, Starlink uses DHCP for IPv4 and SLAAC/DHCPv6-PD for IPv6 to assign the router or client connected directly to the Starlink terminal. Starlink can only assign one IPv4 address per client. IPv6 capable routers will be delegated a /56 prefix for the router to manage. While using the Starlink WiFi router, IP addresses will be assigned to Starlink routers, and the router will NAT all client traffic towards Starlink. The Starlink Gen2 WiFi router is compatible with IPv6 and will assign IPv6 addresses to compatible WiFi or wired clients. Starlink IP addresses are leased for five minutes at a time but that doesn't mean the IP will change every five minutes. Starlink will try to maintain the IP for as long as the device is connected and has a public IP. Public IP addresses are bound to the Starlink device for 24 hours regardless of the DHCP lease time. This ensures that if the Starlink device is rebooted or disconnected for less than 24 hours the IP address will not change. Lastly, the Starlink WiFi router supports both WPA2 and WPA3 security protocols, providing network encryption that meets the ISO standard for internet security.

3. Security Baseline

Infrastructure Details

Number of locations: One. As mentioned above, the hardware for Starlink will remain at the owner's residence. They operate off their cell phones and assigned devices.

IT Asset Inventory

Workstations: Three laptops and three tablets

Servers: Zero

Mobile Devices: 9 smart phones

Network Equipment: Starlink for businesses

Operating System Standards

Windows Version: Windows 11

Password Policy Requirements

Minimum Length: 12 Characters

Complexity Requirement: At least one uppercase letter, at least one lower case letter. At least one number. At least one special character.

Expiration Period: 180 days

Account Lockout Threshold: Three

Required Software

Antivirus

Name: Microsoft defender.

Version: Microsoft defender does not have a version number.

Update Frequency: Microsoft defender continuously updates through Windows Updates.

Firewall

Type: Starlink's built-in firewall for businesses. The firewall function through Network Address Translation (NAT).

Key rules: The NAT firewall blocks unsolicited incoming connections from the internet by default. This is standard for most home and small office routers, and it provides a basic level of protection by not directly exposing devices on your internal network to the public internet.

Other Security Software

Name: Ubiquiti UniFi Dream Machine (UDM) / UniFi Dream Router (UDR) / UniFi Express

Deployment Process

Primary Tool: Group Policy (GP) with Windows Server (Traditional On-Premise)

Secondary Tool: Windows Server Update Services (WSUS)

Testing Protocol

Test Environment Description: Testing will be conducted at the residence the Starlink is located. A dedicated Ubiquiti UniFi Dream Router, configured with the baseline firewall rules, provides

controlled internet access for the test segment. All testing will utilize non-production data and designated test user accounts.

Testing Steps:

1. Password Policy Verification - Attempt to create a new user account with a password shorter than the minimum length
2. Antivirus/Endpoint Protection Verification - EICAR test
3. User Access Control (Least Privilege) Verification - Attempt to install software, modify system-level settings, or access restricted network shares.

Master Image Configuration

Base Image Details

OS Version: Windows 11 Required Updates: As needed from 16 June, 2025 install date.

Included Software

Microsoft Office 365 Applications

Adobe Pro

Microsoft Defender Antivirus

Configuration Settings

Security Settings

All workstations will have Microsoft Antivirus enabled and configured.

All users will need to abide by the password policy.

User account control will be enabled.

Network Settings

Ubiquiti UniFi Dream Router be deployed behind the Starlink router.

Virtual Private Network (VPN) for Remote Access.

Secure Wireless Access.

Patch Management

Patch Testing Protocol

Testing Environment: Testing will be conducted at their residence where their Starlink is located.

Testing Duration: Testing will be completed on Sundays (when the company is closed) for as long as needed.

Patch Window: Schedule will follow Microsoft's monthly deployment.

Emergency Patch Process: Immediately following testing protocol. Notify workers of network connectivity issues.

Verification Process:

Verification Steps

1. Verify patch installation was successful
2. Check system logs for potential errors
3. Conduct Scans
4. Monitor

Implementation Process

Pre-implementation Steps

1. Conduct review of IT infrastructure
2. Define Security Requirements
3. Test hardware, software and network configuration

Post-Implementation Steps

1. Monitor system logs, network traffic and security events
2. User training and awareness
3. Regular review and audits

Rollback Procedure

Trigger Conditions: System crash/performance degradation

Rollback Steps:

1. Notify Owners and office manager
2. Execute rollback to previous state
3. Document all actions during rollback steps and archive for historical records

Allowed Applications

1. Canva
2. Home AI
3. Garden AI
4. Adobe products
5. Quickbooks

Blocked Applications

1. Gaming applications
2. Entertainment applications that don't align with the company's standards or morales
3. Personal cloud storage applications

Encryption Requirements

Encryption Standard: AES-256 & TLS 1.3

Affected Systems: All company owned IT hardware

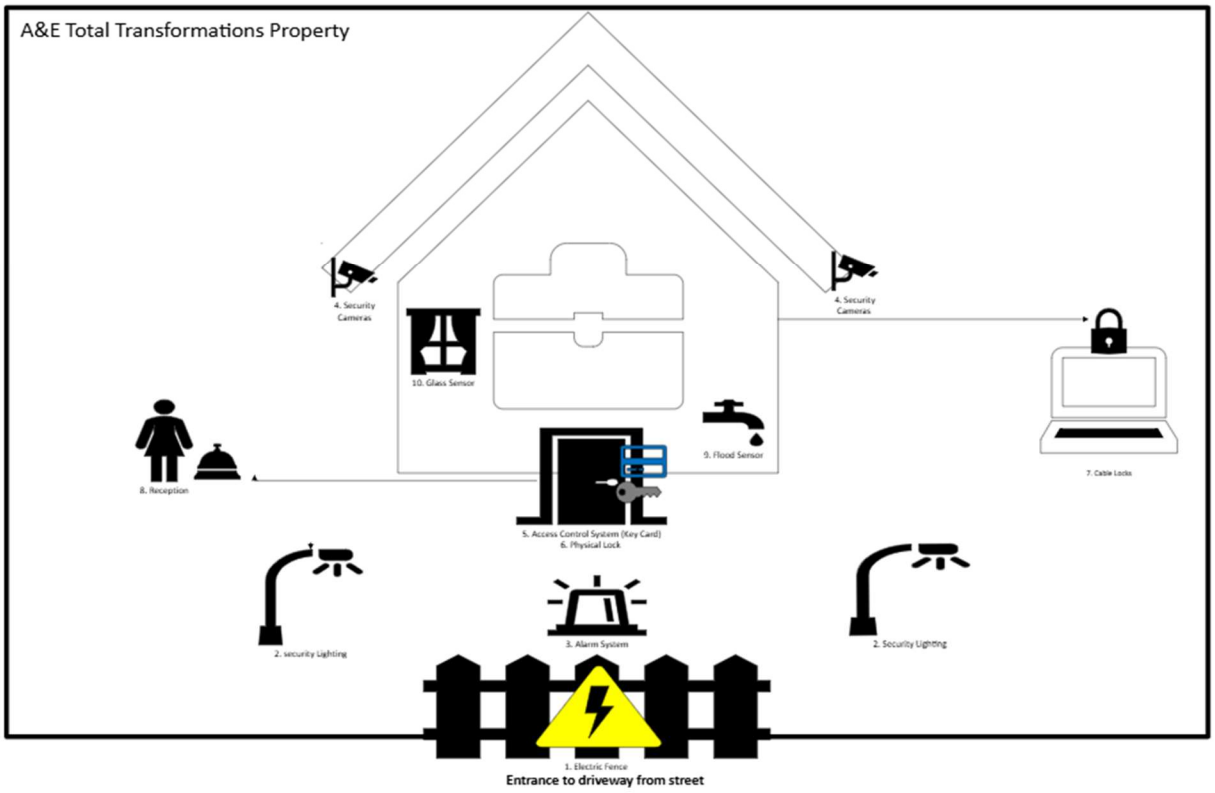
Mobile Device Management

MDM Solution: Microsoft Intune

Controlled applications: All applications on business owned hardware

4. Physical Security

Security Control Layout



Control: Electric Fence

Purpose: A fence around the perimeter of the property will provide a physical security barrier and an extra added obstacle against intrusions.

Security Benefit: This could prevent or delay a break in attempt.

Justify Control Selection and placement: This will establish an effective perimeter security barrier. The fence will be ten feet high and includes shock deterrent with a 7,000 volt.

Control: Security Lighting

Purpose: If someone tries to breach the electronic fence, ultra bright LED lights will be triggered, lighting the entire property up so all elements are visual.

Security Benefit: Deters break in attempts from fear of being seen ultimately adding another incentive to flee.

Justify Control Selection and placement: An intruder does not want attention to their actions, adding another layer of physical security to the fence line that provides light to the entire property will potentially motivate them to leave the property.

Control: Alarm System

Purpose: Constant monitoring. An alarm system provides round-the-clock surveillance.

Security Benefit: A visible security system can deter potential intruders.

Justify Control Selection and placement: Professional alarm system with monitoring allows for quick responses to emergencies.

Control: Security Cameras

Purpose: Record suspicious behavior.

Security Benefit: Continuous recording, advanced analytics, 2-way-talk, remote monitoring, built in sirens and both cloud and on-site storage.

Justify Control Selection and placement: If there was a break in, relevant video footage could be retrieved quickly to identify the intruders.

Control: Access Control Systems (Keycard/ Reader)

Purpose: Keycards for entry and exit authorization.

Security Benefit: Access to certain areas can be permitted to those who are granted access via their keycards.

Justify Control Selection and placement: These will keep a log of dates/times employees enter/exit the property. In the event there is employee misconduct, we can determine who was in the building during the event.

Control: Physical Locks

Purpose: Ensure all exterior doors strong, pick resistant deadbolt locks.

Security Benefit: Only those with physical keys can gain access to the facility.

Justify Control Selection and placement: Common sense security measure that is extremely basic but worth noting.

Control: Cable Locks

Purpose: Lock networking devices to a fixed object.

Security Benefit: Prevents theft of valuable critical assets.

Justify Control Selection and placement: If these assets weren't locked down, a person could easily and quickly steal them.

Control: Reception/Entry Personnel

Purpose: Office manager or other designated staff to sit at the front door of the property.

Security Benefit: Provides active surveillance and can respond immediately to security incidents.

Justify Control Selection and placement: A dedicated person manning the front door can service as a first line defense for vetting visitors.

Control: Flood sensor

Purpose: Notify business of flood threat.

Security Benefit: Allows for immediate action prior to water accumulating and causing significant damage to network equipment and other critical office equipment.

Justify Control Selection and placement: A flood sensor protects network equipment and employee workstations. Having to replace these items can be extremely costly and significantly disrupt daily operations.

Control: Glass break Sensor

Purpose: Detects sound frequencies when glass breaks/shatters.

Security Benefit: Early detection of an intruder.

Justify Control Selection and placement: Alarm will be triggered if glass is shattered. The alarm could deter the intruder from proceeding.

5. Incident Response

Purpose and Objective: A&E Total Transformation's primary purpose of the policy is to detect and contain security incidents while limiting damage and operational disruption. Our objective is to restore our operations as quickly as possible after an incident. While safeguarding client details, financial information and other proprietary information from unauthorized access.

Scope of the Policy: This policy pertains to A&E Total Transformation employees, contractors and guest users. This policy administers the response to cybersecurity incidents affecting A&E Total Transformation's network infrastructure. Which includes, company owned hardware and software as well as network connectivity (Starlink access).

Definition of Security Incidents and Related Terms

Security Incident: An event that results in degradation of A&E Total Transformation's network infrastructure by compromising the integrity or availability of hardware and/or software.

Technical Risks: The potential for an incident to damage or compromise our network infrastructure, hardware, software or data.

Financial Risks: An incident that results in direct financial loss, increased costs or a decrease of revenue.

Human Resource Risks: When an incident can negatively impact the safety, trust, productivity, or morale of our personnel.

Operational Risk: An event that disrupts, hinders or halts daily business operations.

Threat: A circumstance or event that could cause harm to network infrastructure.

Vulnerability: A weakness in our network infrastructure and/or security procedures.

Cyber Attack: An attempt to exploit a vulnerability within our network or business operations in general.

Data Breach: When sensitive or protected dad has been accessed by an unauthorized user.

Phishing: When a hacker is able to manipulate users into revealing sensitive information like a username, password or banking information.

Organizational Structure and Definition of Roles, Responsibilities, and Levels of Authority

Organization Structure:

Name	Privilege Level	Full access to all system settings and sensitive data to ensure network and systems work properly
Lisa Torres	High	Yes
Alex Torres	High	Yes
Victoria Calanche	Medium	No
Kaiden Salazar	Low	No
Kyrine Brown	Low	No
Alana Garcia	Low	No
Sunni Dupris	Low	No
Myrna Davis	Low	No
Jesus Brown	Low	No

Definition and authority of roles:

Privilege Level High (The Incident Response Lead) – The Incident Response Lead is responsible for managing operations during a security incident. The Incident Response Lead holds the highest authority but can delegate as needed.

Privilege Level Medium (Incident Response Assistant) - The Incident Response Assistant reports directly to the Incident Response Lead while assisting with required security incident procedures.

Privilege Level Low (User/Team Member) – Members can be asked to participate on a as needed or required basis per Incident Response Lead's direction.

Requirements for Reporting Incidents:

What to Report

- Suspected cyber-attacks, vulnerabilities, or threats
- Other risks such as financial, technical, operational, environmental or risks w/in the human resources realm

How to Report

Immediately report incidents in person or via mobile phone to:

Lisa Torres 915-244-1397 or Alex Torres 915-244-1398

Prioritization or Severity Rankings of Incidents

Risk Identification:

Risk Name	Risk Type	Note
Client Non-Payment	Financial Risks	When clients fail to pay for services, the business could take a damaging financial hit and have significant debt.
Dependence on Single Technology	Technical Risks	We are relying heavily on Starlink services. If something was to go array with their services, it would hinder our operations.
Data Loss	Technical Risks	If files or data are lost or corrupted the businesses continuity and vital records could be degraded.
Supply Chain Disruption	Operational Risks	The current political climate could directly affect shipments and other logistical needs with our vendors.
Economy/Recession	Financial	A negative financial climate could decrease a demand for services, leading to lower profits.
Fraud	Financial	Employee embezzlement can lead to financial losses.
Workplace Accidents	Human Resources	Injuries can occur in the home construction business and cause a handful of financial and liability issues.
Natural Disasters	Environmental	Flash flooding and severe storms are a known issue in the area and could cause physical damage to equipment and job locations.

Employee Misconduct	Human Resources	Fraud, theft and data mishandling is always a concern. We take pride in hiring the best but know circumstances can change.
Cyber Attack	Technical Risks	A cyber attack could compromise our network and cause technical and financial chaos.

Risk Assessment:

Risk Ranking	Risk Name	Priority Level
1	Client Non-Payment	High
2	Dependence on Single Technology	High
3	Data Loss	High
4	Supply Chain Disruption	Medium
5	Economy/Recession	Medium
6	Fraud	Medium
7	Workplace Accidents	Medium
8	Natural Disasters	Low
9	Employee Misconduct	Low
10	Cyber Attack	Low

Risk Mitigation/Management Strategies:

Risk Name	Preventive Measures/Contingency Plans	Note
Client Non-Payment	Require partial payments upon completion of certain phases of construction	
Dependence on Single Technology	Acceptance of Risk	Will operate off cellular data until new WIFI is secured
Data Loss	Monthly server and file backups	
Supply Chain Disruption	Acceptance of Risk	Commonly used materials will be stocked in advance
Economy/Recession	Acceptance of Risk	
Fraud	Accounting and device monitoring for suspicious activity	
Workplace Accidents	Provide quarterly safety training	
Natural Disasters	Acceptance of Risk	Obtain flood insurance
Employee Misconduct	Provide semiannual employee conduct training	
Cyber Attack	Monitor network on a daily basis, stay on top of updates and patches	

Plan Elements:

Mission: To protect A&E Total Transformation against cyber security attacks to include threats, vulnerabilities, data breaches and phishing.

Strategies and Goals: Through this policy, our primary strategy is clear, transparent and timely communication. By applying these communication efforts as our foundation before and during an event we are confident security incidents will be dealt with head on in a quick and efficient manner. Our primary goal is to minimize degradation to our company's operations by preventing security incidents while staying resilient and abreast of new threats and vulnerabilities.

Organizational Approach to Incident Response: A&E Total Transformation's organizational approach to an incident is to focus on minimizing impact through constant communication throughout our team while maintaining a hyper determination on containing threats.

Metrics for Measuring Incident Response Capability: After incidents have been contained, the team that assisted with the event will meet no later than two business days after the event to discuss the following areas of potential concerns:

- How much time and manpower did this event take
- How many incidents took place during the event
- Total financial and/or revenue losses
- Total equipment/hardware malfunctions and/or losses
- Any and all software vulnerabilities that include data breaches

Once the meeting is concluded, a report will be written by the team lead determining the effectiveness of the Incident Response plan.

Roadmap for Maturing Incident Response Capability

- Finalize and implement Incident Response Plan
- Confirm communication channels are clear
- Administer Semi Annual Security Awareness Training
- Tabletop exercises
- Establish a Vulnerability Management Team

Fit into the Overall Organization

The incident response policy falls in line with our everyday operations. Through this plan, A&E Total Transformation remains vigilant during vulnerabilities and resilient during threats while protecting our business and client's needs and information.

Plan Implementation and Review

Effective Date: July 28, 2025

Review Date: Quarterly (CY) by the second week of each new quarter

6. Security Awareness Training:

1

Phishing & Social Engineering

- Phishing is a cyberattack that leverages email, phone, SMS, social media or other form of personal communication to entice users to click a malicious link, download infected files or reveal personal information, such as passwords or account numbers (Lenaerts-Bergmans, 2023)
- A social engineering attack is a cybersecurity attack that relies on the psychological manipulation of human behavior to disclose sensitive data, share credentials, grant access to a personal device or otherwise compromise their digital security (Lenaerts-Bergmans, 2023)
- https://www.youtube.com/watch?v=gSQgbCo6PAg

3

Password Policy Requirements

- **Minimum Length:** 12 Characters
- **Complexity Requirement:** At least one uppercase letter, at least one lower case letter. At lease one number. At least one special character.
- **Expiration Period:** 180 days
- **Account Lockout Threshold:** Three

Good Example: Pluto@Mars!82193
Bad Example: Abc123!

Physical Security of Devices

- Lock your screen
- Physically Lock building and applicable gates
- Keep devices on your person
- Report Lost or Stolen Devices immediately
- Don't let others use your devices

5

Data Handling & Privacy

- You will have access to sensitive company and client data
  - Encrypt Sensitive Data with a strong password before sending
  - Do not share business or client data to

https://youtu.be/N8xEgSe5RwE?si=69V93L1jGSUFHajH

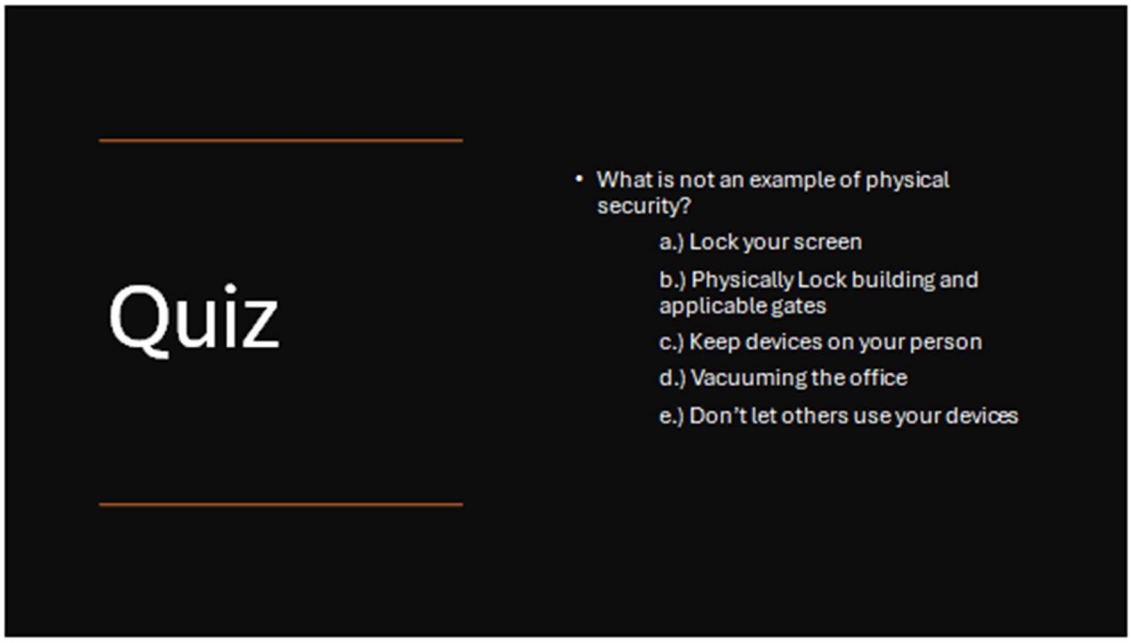
Malware & Software Updates

- Malware (malicious software): Viruses, trojans, spyware, and worms. Malware typically infects a personal computer (PC) through e-mail, Web sites, or attached hardware devices. Mobile malware, including spyware and ransomware, attacks smartphones and tablets, often through text messages and mobile apps (Hosch, 2025)
- Software Updates: https://youtu.be/sEnQ_cNsAW0?si=zPT5E0b5vY9-8C9c

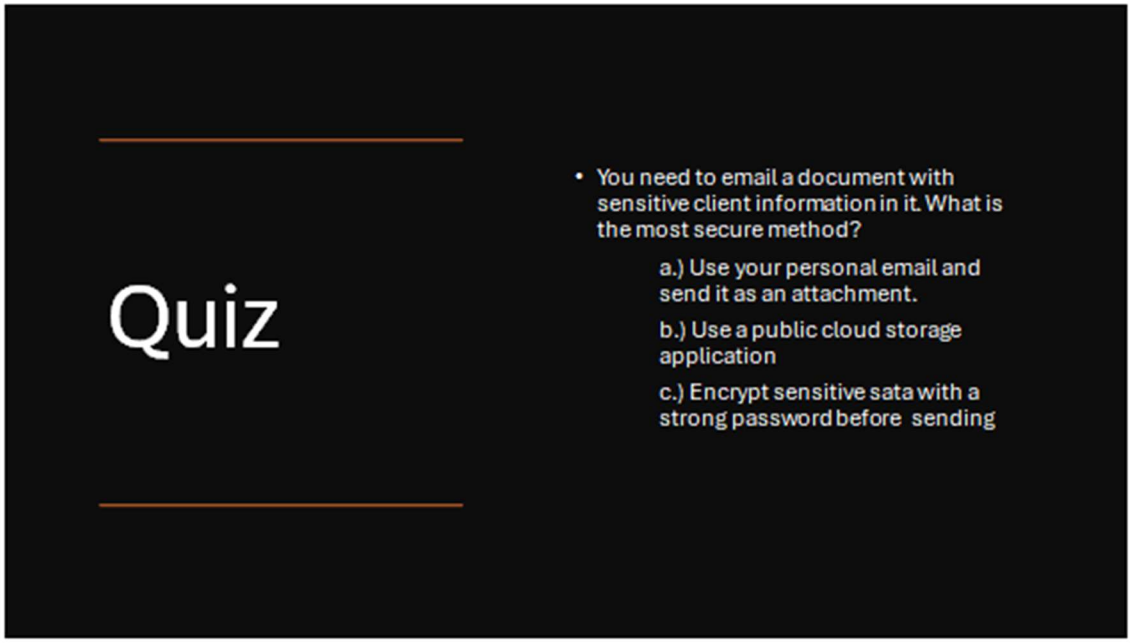
7

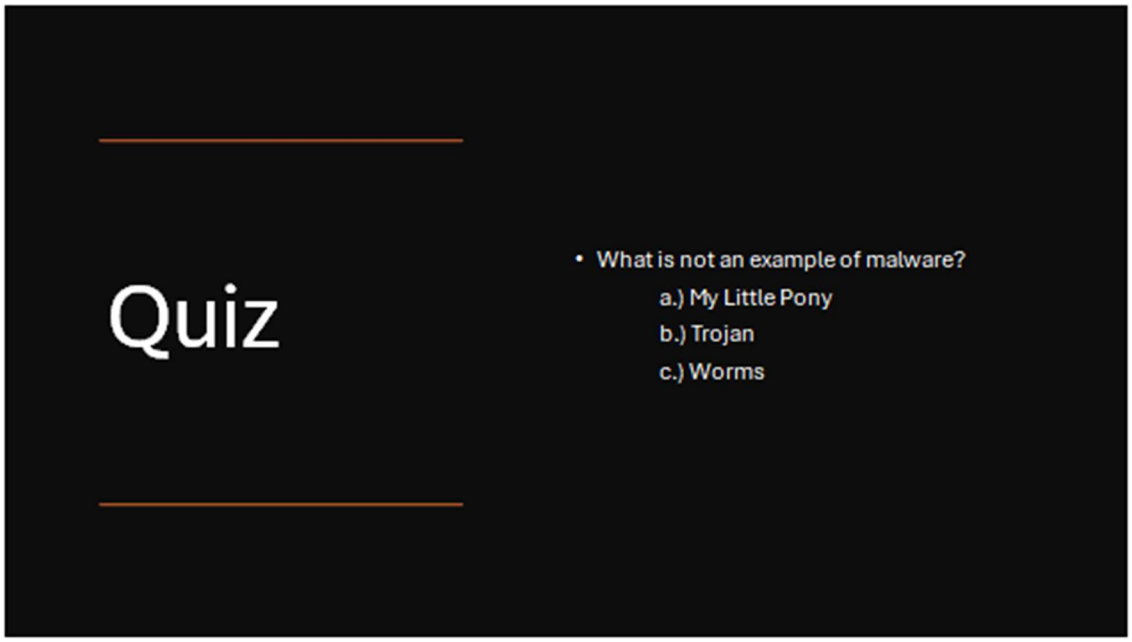
Quiz

- Which of the following meets the minimum password requirements?
  - a.) LoveMyJob123
  - b.) 1234Abcde
  - c.) N0hAck3r!753951@


Quiz
• What is not an example of physical security?
a.) Lock your screen
b.) Physically Lock building and applicable gates
c.) Keep devices on your person
d.) Vacuuming the office
e.) Don't let others use your devices

9


Quiz
• You need to email a document with sensitive client information in it. What is the most secure method?
a.) Use your personal email and send it as an attachment.
b.) Use a public cloud storage application
c.) Encrypt sensitive sata with a strong password before sending



11

Sign In Sheet

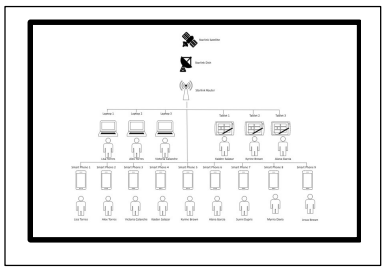
Date of Training:
Instructor Name:

Attendees Printed Name	Signature

7. BYOB Agreement

ACTION REQUIRED: Read, initial each page and sign this document as your acknowledgment and agreement of compliance. Once this is signed and approved by management, you will be granted access to our Starlink service.

For Reference: Current network structure w/issued workstations, tablets and smartphones.



Bring your Own (BYOD) Policy

1) Scope

a) Purpose of BYOD Policy

i) This BYOD policy regulates using personal devices within A&E Total Transformations network. Personal devices include smartphones and tablets. This policy will enforce balance while enabling convenience of BYOD within the required security setting to protect company data while ensuring compliance with regulatory compliance. A&E Total Transformations has nine employees, who will be issued company phones. This should hopefully decrease the need to BYOD. But in the event an individual still requires an option to BYOD the following policy needs to be abided by.

b) Scope of the policy (who and what it applies to)

i) This policy applies to all employees, contractors, and third-party collaborators who use personal devices for work-related tasks. It includes any access to company resources via these devices, whether through A&E Total Transformation's Wi-Fi.

2) Device Eligibility

a) Acceptable devices allowed under this policy.

i) Personal devices allowed under this policy include smartphones, tablets and laptops that meet the following requirements.

(1) iOS 17 and above and/or macOS Sonoma 14 and above

(2) iPhone 15 and above

(3) iPad Pro

(4) iPad Air

(5) MacBook Air

(6) MacBook Pro

b) Minimum requirements for devices (e.g., software versions, security features)

i) Devices must be operating in accordance with above hardware and software configurations. Devices must support MDM software (Microsoft Intune) provided by the company.

3) Enrollment and Registration

a) Process for enrolling personal devices in the BYOD program.

i) Employees and other applicable individuals must use the company's Mobile Device Management (MDM) system to enroll their devices. This involves:

(1) Installation of the MDM Software (Microsoft Intune)

(2) Initial device security configuration

b) Required information for registration(e.g., device details, ownership)

i) The following information is required to registration:

(1) Device, make, model, and serial number

(2) Ownership confirmation (e.g., owned by the employee).

(3) Agreement to this policy that A&E Total Transformations can monitor your device(s)

4) Security Requirements

a) Mandatory security measure (e.g., passcode, encryption, antivirus software).

i) Enrolled devices will comply will the following security measures:

(1) Passcode or biometric lock. Password policy requirements are as follows:

Minimum Length: 12 Characters

Complexity Requirement: At least one uppercase letter, at least one lower case letter. At least one number. At least one special character.

(2) Full device encryption (default on iOS). FileVault required for Macs.

(3) Antivirus software (default on Apple products)

(4) Device configuration and management through MDM software (Microsoft Intune) to enforce remote wipe.

b) Device configuration and management through MDM (Microsoft Intune)

i) MDM software enforces device settings, monitors compliance, and applies security patches. It also enables remote actions such as locking or wiping devices.

c) Procedures for reporting lost or stolen devices.

i) If a device is lost or stolen, the employee must immediately report it to A&E Total Transformation Owners: Lisa Torres and/or Alex Torres. Your device will be remotely wipe.

5) Acceptable Use

a) Guidelines for appropriate use of personal devices for work purposes.

i) Per A&E Total Transformation' acceptable use policy, personal devices may be used for work-related tasks like, document sharing and accessing application needed to perform job related duties.

b) Prohibited activities and behaviors.

i) The following is prohibited:

(1) Installing unauthorized or pirated software

(2) Bypassing MDM controls

(3) Accessing inappropriate or illegal content using a work network.

c) Consequences of violating the acceptable use guidelines

i) Depending on the severity of the violation, violations may result in the revocation of BYOD privileges, disciplinary action, or termination of employment.

6) Data Ownership and Privacy

a) A&E Total Transformations' ownership and control over work-related data on personal devices.

(i) A&E Total Transformations' retains ownership of all work related data stored or accessed via personal devices.

b) Employee's responsibility to protect confidential information.

(i) Employees must ensure that work-related data is protected and cannot be accessed by unauthorized individuals.

c) A&E Total Transformations' right to access, monitor, and retrieve data on personal devices.

i) A&E Total Transformations reserves the right to access, monitor, and retrieve work-related data on personal devices as necessary to ensure compliance with this policy.

7) Support and Maintenance

a) Scope of technical support provided by the company for personal devices.

i) A&E Total Transformations will provide limited support for the company's applications and MDM software issues.

b) Employee's and applicable individuals' responsibilities for device maintenance and updates.

i) Employees and applicable individuals are responsible for ensuring their devices remain in good working order, including updating their operating systems and maintaining antivirus protection.

c) Procedures for troubleshooting and resolving issues.

i) Employees and applicable individuals must contact A&E Total Transformations for troubleshooting assistance with any business-related applications or MDM issues.

8) Compliance and Enforcement

a) Employees and applicable individuals must acknowledge and agree to comply with this BYOD policy.

i) Employees and applicable individuals must initial all pages of policy and agree to comply fully to referenced terms.

b) A&E Total Transformations right to enforce this policy and take disciplinary action for violations.

i) A&E Total Transformations reserves the right to enforce compliance with this policy by monitoring access revocation and taking disciplinary action.

c) Process for reporting policy violations or security incidents.

i) A&E Total Transformations owners, Lisa Torres and/or Alex Torres must be notified of any security incidents or violations of this policy within 12 hours.

9) Liability and Disclaimer

a) A&E Total Transformations limitation of liability for damage or loss of personal data.

i) A&E Total Transformations is not liable for any damage or loss of personal data resulting from using a personal device for work.

b) Employees and applicable individuals' assumption of risk when using personal devices for work.

i) Employees and applicable individuals accept full responsibility for any risk of using personal devices for work purposes

10) Policy and Review Updates

a) Statement of individuals understanding and agreement to the BYOD policy.

i) By initialing each page and signing below I hereby acknowledge and agree to comply with the terms of the BYOD policy.

b) Signature and date for individual acknowledgment

Printed Name: _____

Signature: _____ Date: _____

Internal Use

11) Received by and network information

a) Brief individual on Starlink connection process

b.) Scan and save file to electronic filing system, email a copy to HR firm.

Printed Name: _____

Signature: _____ Date: _____