

Assignment 5: Security Policy Strategies

CYBR3080 – IT Service Delivery Security

Gregory Stephens

Mobile and Remote Work Security Policy Report for Trinity Systems

As companies more and more embrace hybrid and totally remote work setups, guaranteeing data security in dispersed environments becomes vital. The guidelines provide steps to safeguard sensitive data, assure compliance with sector standards, and reduce mobile- and remote-work related cyber risks.

This policy's value is in allowing staff members to work effectively from any location while at the same time protecting Trinity Systems' intellectual property, customer data, and operational integrity. Since remote employees are frequently hit by cybercriminals using phishing attacks, unsecured Wi-Fi networks, and device weaknesses, this plan is a proactive defensive strategy (Critical Insight, 2023). It also fits with Trinity Systems promise to promote confidence among consumers using our cloud infrastructure for their operations.

Business-Aligned Approach

The business-aligned approach emphasizes the direct integration of security measures with corporate objectives and operations. This method guarantees that security projects support business continuity, increase productivity, and fit Trinity Systems' goal of offering dependable cloud solutions.

Reasoning behind the selection of the business-aligned approach:

- 1. Relationship with Organizational objectives:* A business-aligned approach gives first priority to techniques that support Trinity Systems' primary objectives—providing advanced cloud technology while keeping strict security standards.
- 2. Cost-Effectiveness:* Customizing security measures to particular company needs helps to avoid unnecessary spending on unnecessary equipment or procedures.
- 3. Design centered on employees:* Considering user experience helps staff members to follow the rules without sacrificing performance.
- 4. Adaptability:* Trinity Systems growth is supported by the business-aligned approach with flexible changes to the rules based on changing business needs.
This method guarantees assets are safeguarded while enabling smooth cooperation and creativity since every part of the policy from access control to personnel training is planned with this goal in mind.

Key Elements of the Policy

1. *Secure Access for Mobile and Home Devices*

- Access for home as well as mobile tools is locked regardless of location, all access to corporate systems must be subjected to multi-factor authentication (MFA).
- All devices—whether provided by the business or personal use—they should satisfy minimum security criteria including current antivirus software and firewalls (ClickArmor, 2023).
- Suggest the use of virtual private networks (VPNs) to secure data transmission and forbid access to company resources via unsecured public Wi-Fi.

2. *Data Protection in Remote Environments*

- Using sophisticated encryption algorithms (SentinelOne, 2023), encrypt any sensitive information on mobile devices or being sent during remote work sessions kept on mobile devices.
- To keep unattended devices from being unauthorized accessed at home or in public areas, apply automatic screen lock and timeout features on all devices.
- Unless clearly authorized and encrypted, limit the downloading or storing of sensitive corporate data on personal devices.

3. *Employee Training and Awareness for Remote Work*

- Every quarter, provide required cybersecurity training emphasizing the dangers of remote work, including but not limited to phishing attacks, unsafe Wi-Fi use, and social engineering strategies (Critical Insight, 2023).
- Offer employees simulated phishing drills so they may identify and react to malicious emails directed at remote staff (SentinelOne, 2023).
- Share a brief "Remote Work Security Checklist" listing actions for keeping secure habits, including device locking, alerting authorities of strange behavior, and safeguarding home Wi-Fi networks (ClickArmor, 2023).

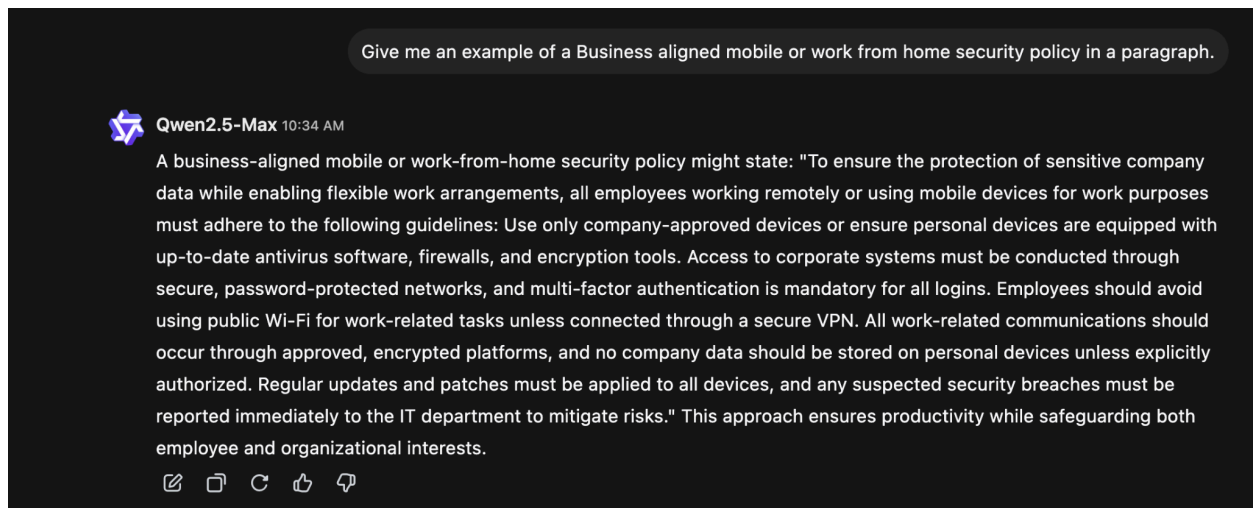
References

ClickArmor. (2023). 7 remote work cyber security rules every business should follow. Retrieved from <https://clickarmor.ca/7-remote-work-cyber-security-rules-every-business-should-follow/>

Critical Insight. (2023). 8 best practices for working remotely. Retrieved from <https://www.criticalinsight.com/blog/8-best-practices-for-working-remotely>


SentinelOne. (2023). Remote working security risks. Retrieved from <https://www.sentinelone.com/cybersecurity-101/cybersecurity/remote-working-security-risks/>

Qwen 2.5 Max. (2025) Prompt used:



The screenshot shows a chat interface with a dark background. At the top, a light gray rounded rectangle contains the prompt: "Give me an example of a Business aligned mobile or work from home security policy in a paragraph." Below this, the model's response is shown, preceded by a purple Qwen logo and the text "Qwen2.5-Max 10:34 AM". The response is a paragraph of text. At the bottom of the response, there are five small icons: a pencil, a square, a circular arrow, a thumbs up, and a thumbs down.

Give me an example of a Business aligned mobile or work from home security policy in a paragraph.

 **Qwen2.5-Max** 10:34 AM

A business-aligned mobile or work-from-home security policy might state: "To ensure the protection of sensitive company data while enabling flexible work arrangements, all employees working remotely or using mobile devices for work purposes must adhere to the following guidelines: Use only company-approved devices or ensure personal devices are equipped with up-to-date antivirus software, firewalls, and encryption tools. Access to corporate systems must be conducted through secure, password-protected networks, and multi-factor authentication is mandatory for all logins. Employees should avoid using public Wi-Fi for work-related tasks unless connected through a secure VPN. All work-related communications should occur through approved, encrypted platforms, and no company data should be stored on personal devices unless explicitly authorized. Regular updates and patches must be applied to all devices, and any suspected security breaches must be reported immediately to the IT department to mitigate risks." This approach ensures productivity while safeguarding both employee and organizational interests.

