Harris McCall

10/15/2023

Lab #3

XYZ Corporation

Mobile Device Security Policy

Effective date: 06/15/2023

Approved by:

Jack Donaghy - Chief Information Officer

06/15/2023

1. Introduction

XYZ Corporation recognizes the increasing importance of mobile devices in today's business environment. Mobile devices, including smartphones, tablets, and laptops, play a vital role in facilitating remote work, enhancing productivity, and improving communication. However, the use of mobile devices also presents significant security risks to our organization. This Mobile Device Security Policy aims to establish guidelines and best practices to safeguard XYZ Corporation's sensitive data, information, and network infrastructure.

2. Scope

This policy applies to all employees, contractors, consultants, and any other personnel who use mobile devices to access XYZ Corporation's resources and data. It encompasses all company-owned or personally owned mobile devices that connect to the corporate network, systems, or handle company data. This policy also applies to all operating systems and platforms used on mobile devices, including but not limited to iOS, Android, MacOS, and Microsoft Windows.

3. Policy

3. 1 Technical Requirements - XYZ Corporation implements the following technical requirements to ensure the security of mobile devices:

- ***Device Encryption -*** All mobile devices must enable encryption for data at rest. This includes full-disk encryption for laptops and device-level encryption for smartphones and tablets. XYZ Corporation's IT department will provide guidance on enabling encryption for personally owned devices.
- ***Authentication and Access Control -*** Mobile devices must use strong, unique passwords, PINs, or biometric authentication methods, and too many failed login attempts should trigger a device full-wipe and reset. Users should also enable auto-lock functionality with a short inactivity timer. Note that personally owned devices will be given less permissions than company owned devices, and a company owned device may be required to access certain resources.
- ***Remote Wipe and Tracking -*** GPS tracking should be enabled on all mobile devices to aid in recovery, and all mobile devices must be configured to support remote wipe capabilities in case recovery of a lost device is impossible.

- ***Application Whitelisting -*** Only approved and authorized applications are permitted to run on mobile devices. Users are not allowed to install or use unauthorized applications on company-owned devices.
- ***Secure Connectivity -*** Mobile devices must connect to the corporate network and resources via secure and authenticated VPNs when accessing sensitive data. Employees must use secure, trusted Wi-Fi networks, and avoid open, unsecured public Wi-Fi. Lastly, Bluetooth and Wi-Fi connections should be disabled when not in use.

3.2 User Requirements - XYZ Corporation expects employees to follow these guidelines for using mobile devices:

- ***Reporting Lost or Stolen Devices -*** In the event of a lost or stolen mobile device, users must immediately report the incident to the IT department and, if applicable, their supervisor. The device will be remotely wiped, if necessary, to prevent unauthorized access.
- ***Data Handling -*** Employees should store sensitive data on company-approved cloud storage or network drives rather than on the device itself. Sensitive data should be encrypted when transmitted over the internet.
- ***Software Updates -*** Users must keep their mobile device's operating system and applications up to date with the latest security patches and updates.
- ***Phishing Awareness -*** Employees should exercise caution and be aware of phishing attempts, particularly on mobile devices. If they encounter a suspicious message or link, they should report it to the IT department.
- ***Physical Security -*** Employees should not leave mobile devices unattended in public places. Laptops should be securely stored when not in use, and smartphones and tablets should be protected from theft.

4. Compliance

XYZ Corporation takes mobile device security seriously, and all employees are expected to comply with this policy. Failure to adhere to these guidelines may result in disciplinary action, up to and including termination of employment.

5. Policy Review

This Mobile Device Security Policy is subject to regular review and updates to adapt to evolving security threats and technology changes. All employees are responsible for staying informed about policy changes and abiding by the latest requirements.

6. Help Desk Support

For assistance or to report mobile device-related issues, employees can reach the help desk via the following contact methods:

- Help Desk Phone: 987-456-3215
- Help Desk Email: internal.support@xyz.org
- Help Desk Ticketing System: internal.helpdesk.org/submit-a-ticket.html

Employees are encouraged to reach out to the help desk promptly for any mobile device-related concerns or questions. The help desk is available during regular business hours to provide support and guidance.

7. Employee Acknowledgement and Acceptance

The employee who signs below attests that they have read, understood, and agree to comply with the guidelines within XYZ Corporation's Mobile Device Security Policy. The employee accepts all responsibility for adhering to the measures outlined in this policy:

Print Name: _____

Signature: _____

Date: _____

References

Columbia Basin College. (2019, July). *Columbia Basin College Online Privacy Policy*. Retrieved from www.columbiabasin.edu: https://www.columbiabasin.edu/public-info/privacy-policy/index.html

Howell, G., Franklin, J., Sritapan, V., Souppaya, M., & Scarfone, K. (2023). *NIST SP 800-124r2: Guidelines for Managing the Security of Mobile Devices in the Enterprise.* Gaithersburg, Maryland: National Institute of Standards and Technology.