Student:	Email:
Kanchan Chopde	hq0656@wayne.edu

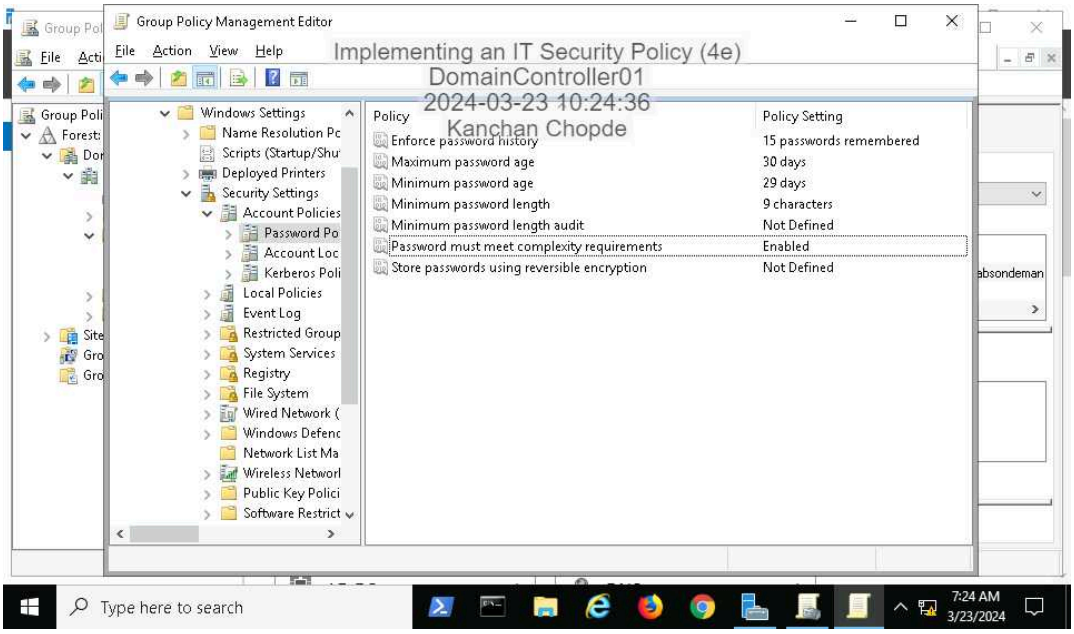
Time on Task:	Progress:
1 hour, 36 minutes	100%

Report Generated: Saturday, March 23, 2024 at 7:42 PM

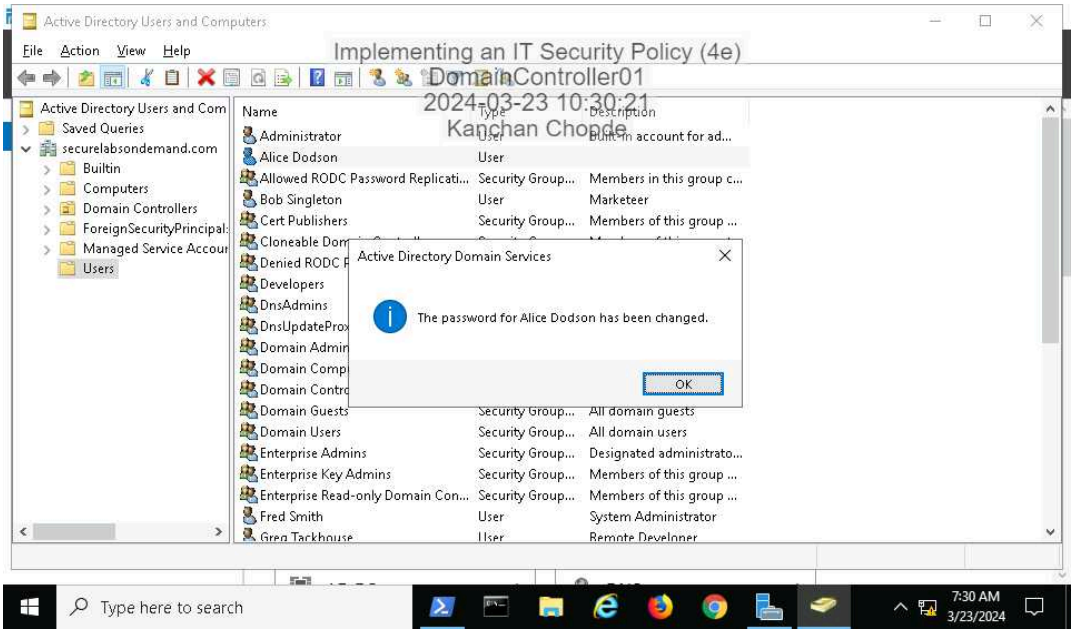
Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

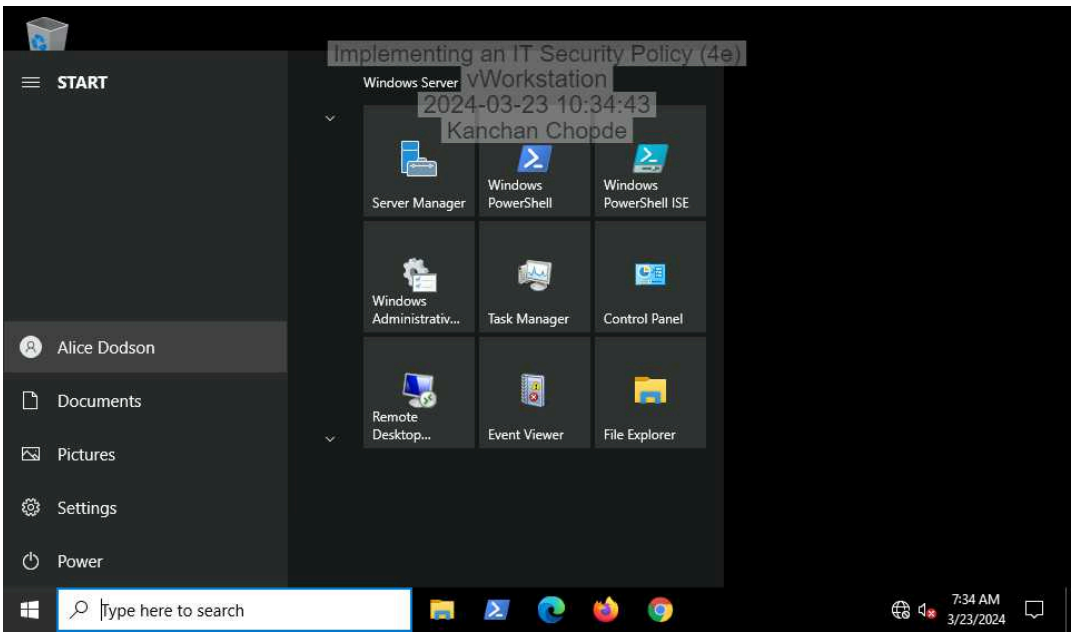
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



28. **Make a screen capture** showing the **successful password change message**.

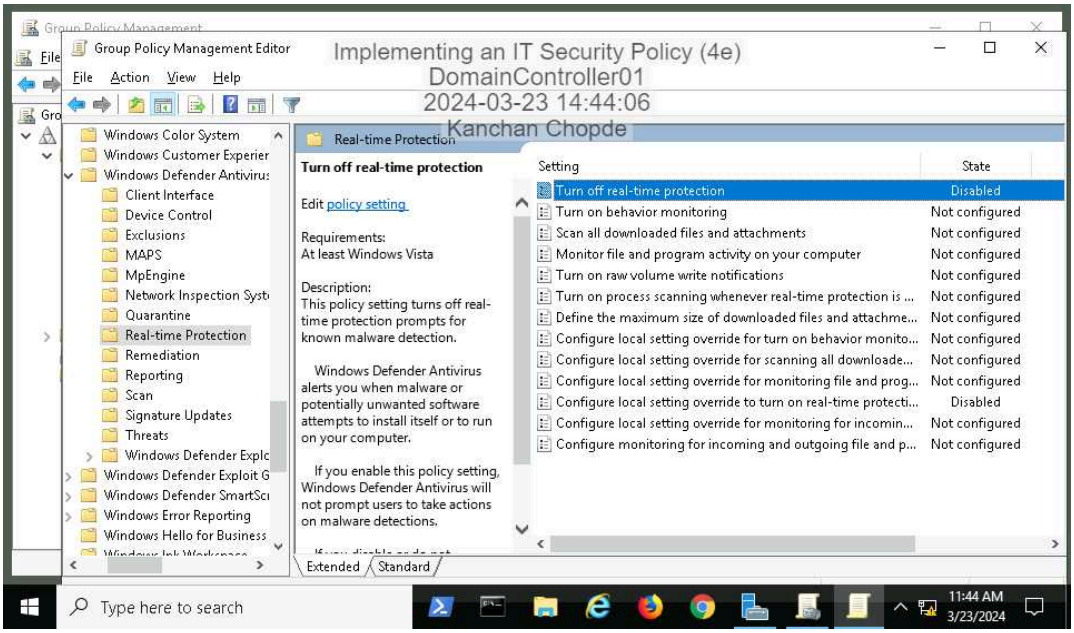


36. **Make a screen capture** showing the **logged on user account**.

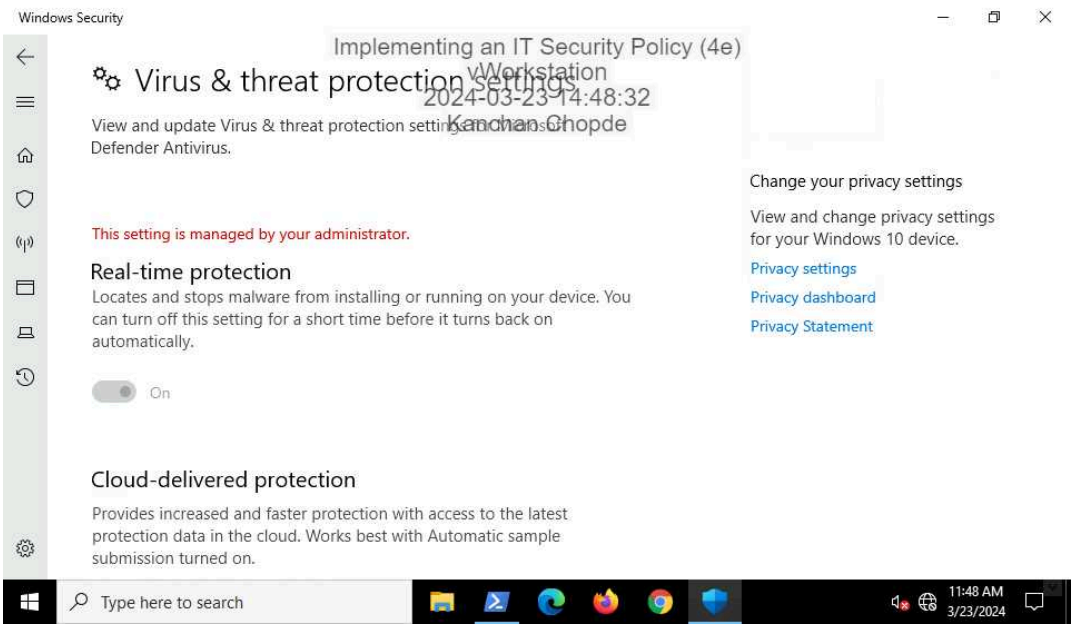


Part 2: Implement an Antivirus Policy

16. **Make a screen capture** showing the **newly configured Domain Real-time protection Policy settings.**



25. **Make a screen capture** showing the **grayed-out real-time threat protection settings**.

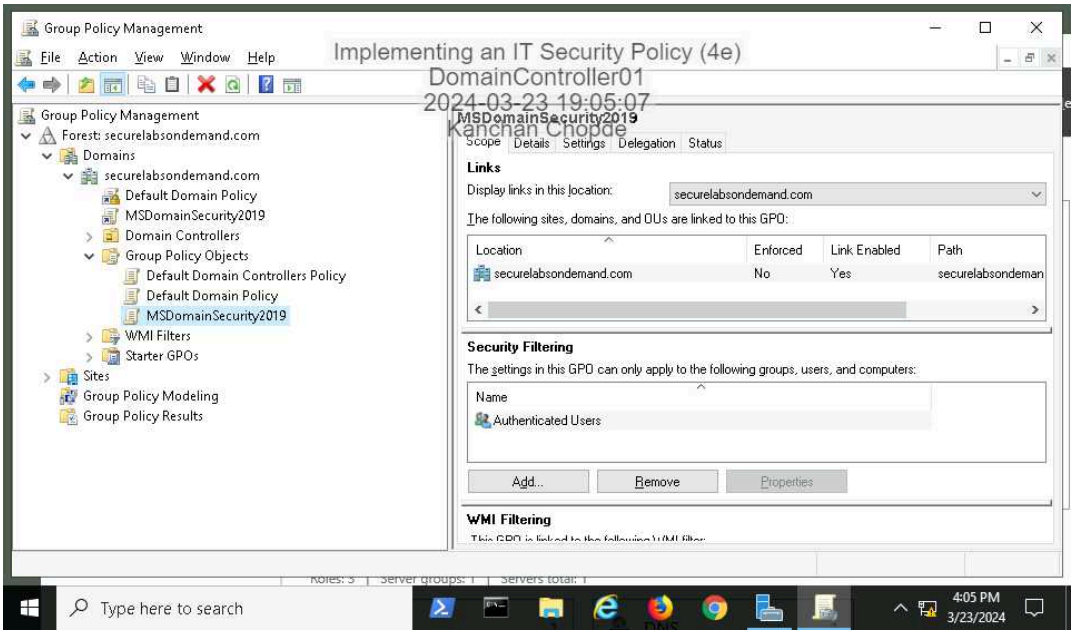


Section 2: Applied Learning

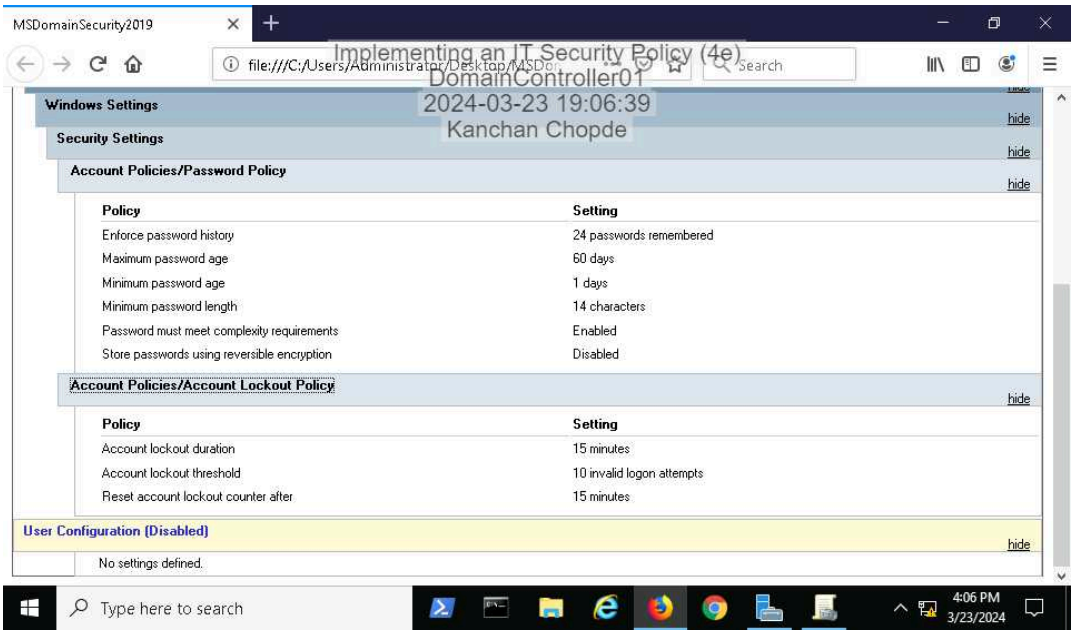
Part 1: Apply a Windows Security Baseline

6. **Make a screen capture** showing **Microsoft's recommended Password and Account Lockout policy settings**.

19. **Make a screen capture** showing the **linked MSDomainSecurity2019 object**.

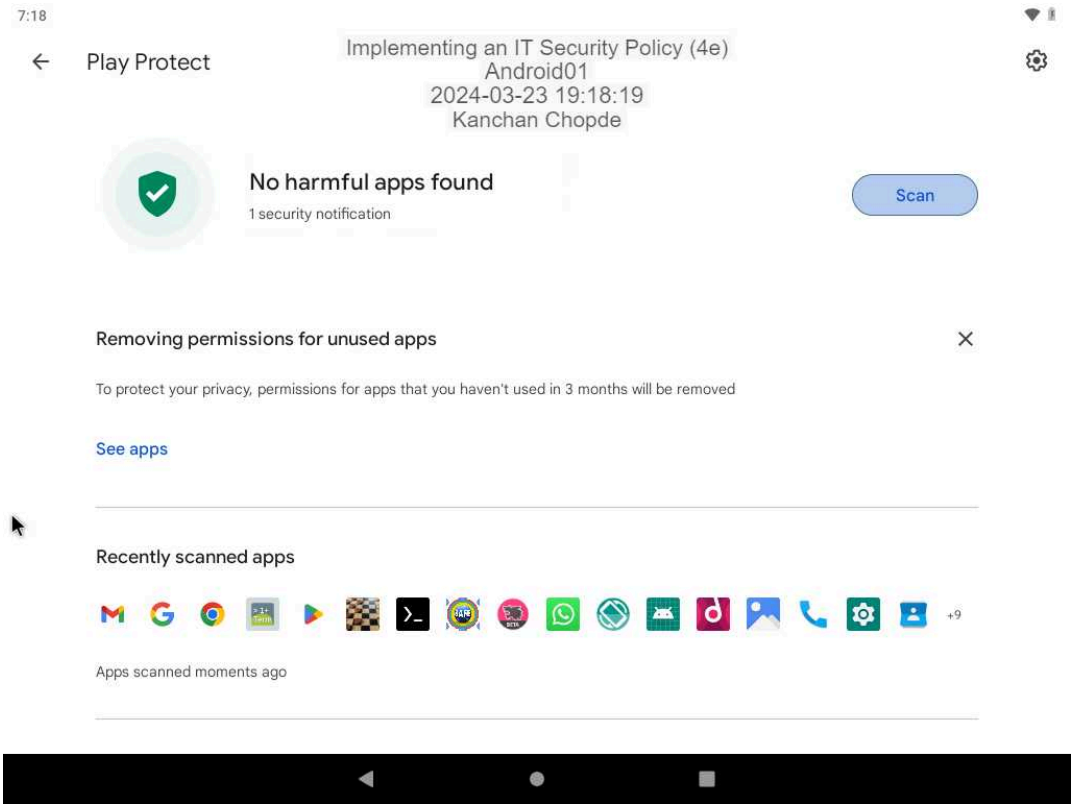


23. **Make a screen capture** showing the **Password and Account Lockout policy settings**.

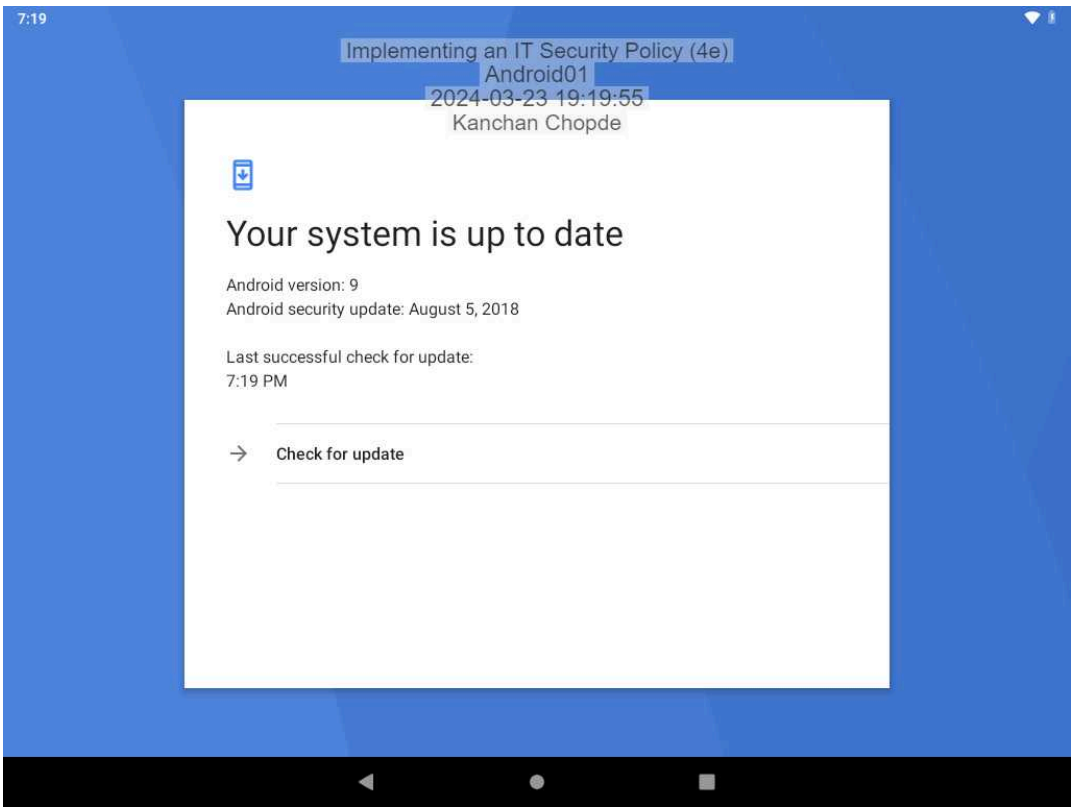


Part 2: Implement a Mobile Device Security Policy

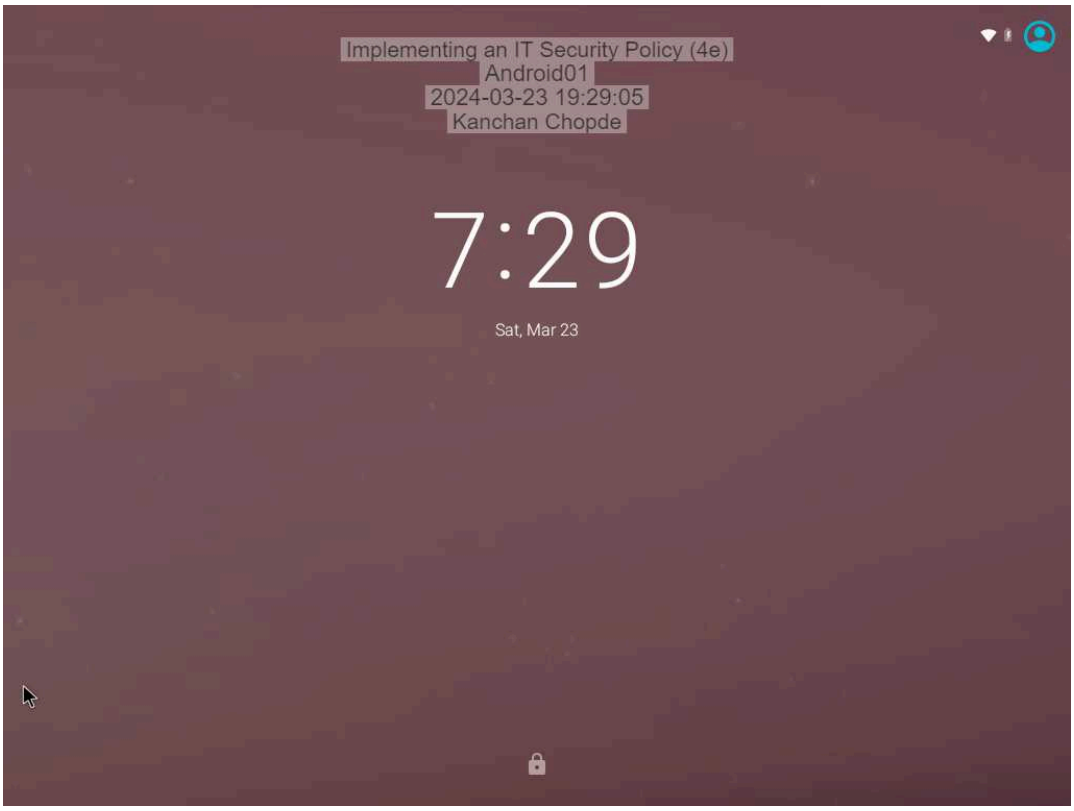
7. **Make a screen capture** showing the **results of the Google Play Protect scan**.



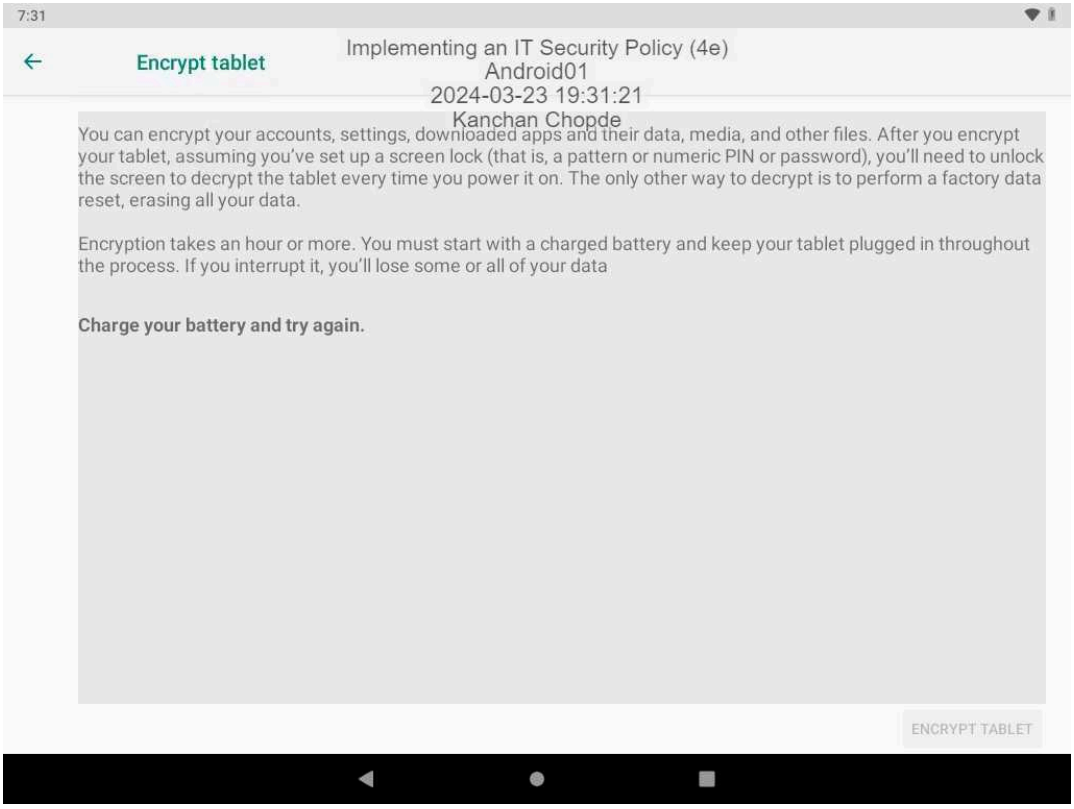
11. **Make a screen capture** showing the **updated "last successful check for update" timestamp**.



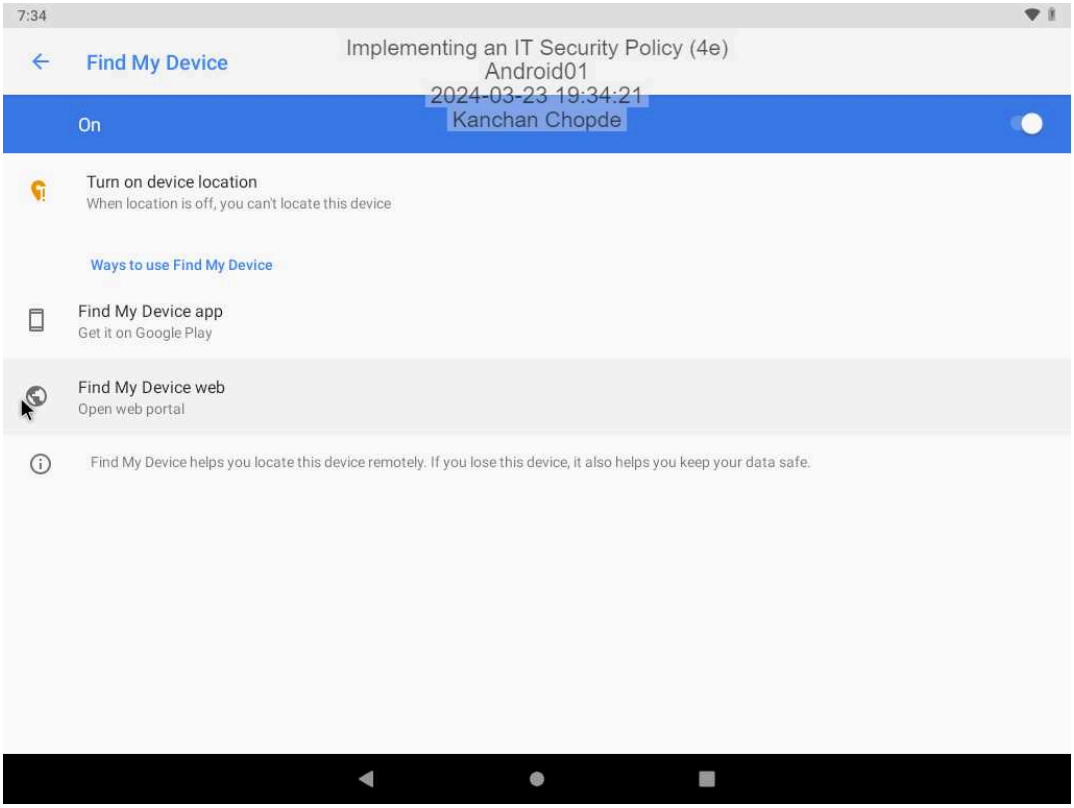
19. **Make a screen capture** showing the **Android lock screen**.



25. **Make a screen capture** showing the **encryption set-up explanation**.



27. **Make a screen capture** showing the **Find My Device settings**.



Section 3: Challenge and Analysis

Part 1: Research Acceptable Use Policies

Using the Internet, **research** Acceptable Use Policies, then **identify** at least five common policy statements and **explain** their significance. Be sure to cite your sources.

Acceptable Use Policies (AUPs) are crucial documents that outline the acceptable behaviors and activities for users of a particular system, network, or service. They are essential for maintaining security, privacy, and ethical standards within an organization or community. Here are five common policy statements found in AUPs and their significance:

Prohibition of Unauthorized Access: This statement prohibits users from attempting to access systems, networks, or data without proper authorization. Unauthorized access can lead to security breaches, data theft, and compromise of sensitive information. By explicitly prohibiting such actions, organizations can mitigate the risk of unauthorized access and maintain the integrity of their systems.
Responsibility for Security: AUPs often emphasize the responsibility of users to maintain the security of their accounts, passwords, and personal information. Users may be required to follow best practices for password management, report security incidents promptly, and adhere to security protocols established by the organization. This helps minimize the risk of security breaches and ensures that users actively contribute to the overall security posture of the organization.
Restrictions on Offensive Content: AUPs often include clauses prohibiting the creation, transmission, or storage of offensive or inappropriate content. This helps create a professional and respectful environment within the organization and prevents harassment, discrimination, or other forms of misconduct. Additionally, restricting offensive content can help uphold the organization's reputation and avoid legal liabilities.
Usage Limitations: AUPs typically specify usage limitations such as bandwidth restrictions, restrictions on excessive use of resources, or limitations on activities that may disrupt the normal operation of systems or networks. These limitations help ensure fair and equitable access to resources for all users and prevent abuse or misuse that could degrade system performance for others.
Protection of Intellectual Property: Many AUPs include statements regarding the protection of intellectual property rights, such as copyrights, trademarks, and patents. Users are typically prohibited from engaging in activities such as unauthorized distribution of copyrighted material, software piracy, or infringement of intellectual property rights. These provisions help safeguard the organization's assets and prevent legal issues related to intellectual property violations.
These are just a few common examples of policy statements found in Acceptable Use Policies. Each organization may have variations or additional clauses tailored to its specific needs and requirements. (Ref: Cisco, "Acceptable Use Policy (AUP) Guidelines", Purdue University, "Information Technology Resource Acceptable Use Policy", University of California, Berkeley, "UC Berkeley Campus Information Technology Acceptable Use Policy")

Part 2: Research Privacy Policies

Using the Internet, **research** user Privacy Policies, then **identify** at least five common policy statements and **explain** their significance. Be sure to cite your sources.

Privacy Policies are essential documents that outline how an organization collects, uses, discloses, and protects the personal information of its users or customers. Here are five common policy statements found in Privacy Policies and their significance:

Data Collection and Use: This statement explains what types of personal information the organization collects from users and how it is used. It may include information such as names, contact details, payment information, and browsing history. Significance: By being transparent about data collection and use practices, organizations build trust with users and ensure compliance with privacy laws and regulations.

Data Sharing and Disclosure: Privacy Policies often detail whether and how the organization shares users' personal information with third parties. This may include sharing with service providers, partners, or in response to legal requests. Significance: Users have the right to know who their information is being shared with and for what purposes, helping them make informed decisions about using the service or platform.

Security Measures: This statement outlines the security measures implemented to protect users' personal information from unauthorized access, disclosure, alteration, or destruction. It may include encryption, access controls, regular security audits, and employee training. Significance: Demonstrating a commitment to security reassures users that their data is being handled responsibly and reduces the risk of data breaches or cyberattacks.

User Rights and Choices: Privacy Policies often inform users about their rights regarding their personal information, such as the right to access, correct, or delete their data. Additionally, they may explain how users can opt-out of certain data collection or marketing activities.

Significance: Empowering users with control over their data enhances transparency and accountability, fostering a positive relationship between the organization and its users.

Policy Updates and Notification: This statement describes how the organization will notify users of changes to the Privacy Policy and when those changes will take effect. It may include methods such as email notifications, website banners, or pop-up alerts. Significance: Keeping users informed about changes to the Privacy Policy ensures transparency and gives them the opportunity to review and understand any updates that may impact their privacy rights.

These common policy statements serve to protect users' privacy rights, establish trust, and ensure compliance with privacy laws and regulations.

(Ref: "Privacy Policy Best Practices" by TrustArc, "Creating an Online Privacy Policy" by the Federal Trade Commission (FTC), "Privacy Policy Guide" by the International Association of Privacy Professionals (IAPP))