

Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

Student:

Matias Kun

Email:

rwh4zx@virginia.edu

Time on Task:

2 hours, 48 minutes

Progress:

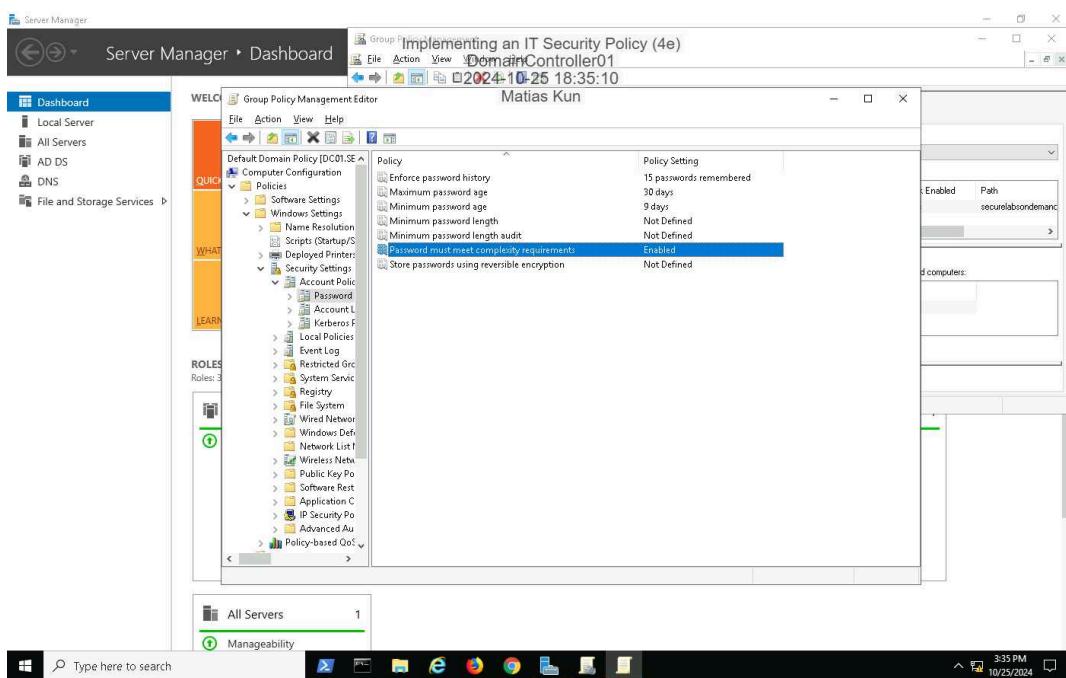
100%

Report Generated: Tuesday, October 29, 2024 at 12:16 PM

Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

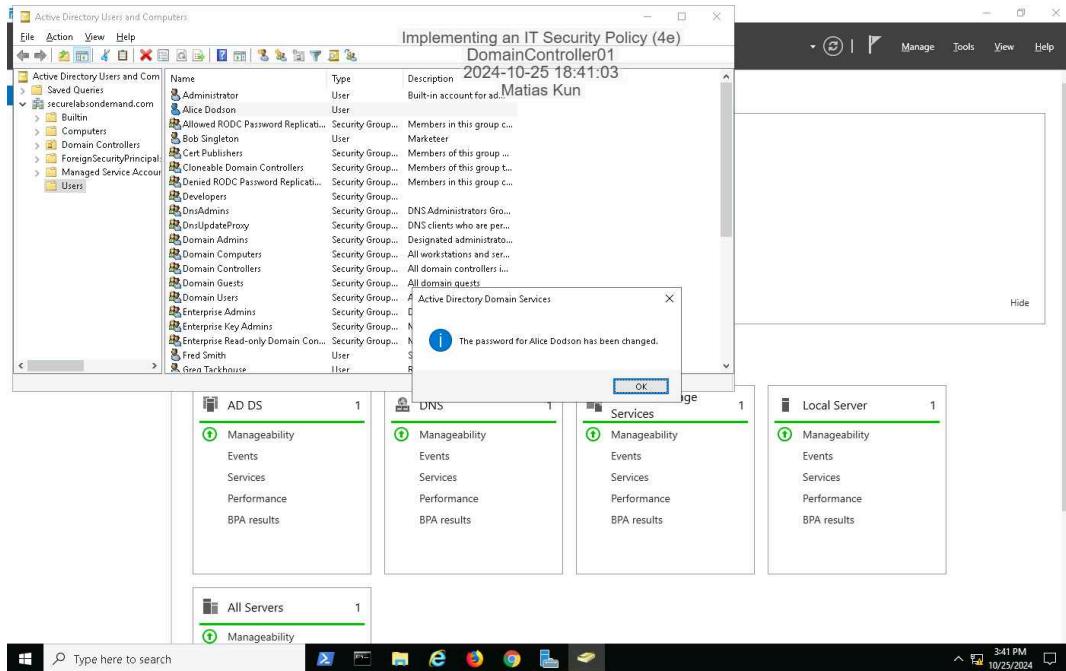
16. Make a screen capture showing the newly configured Domain Password Policy settings.



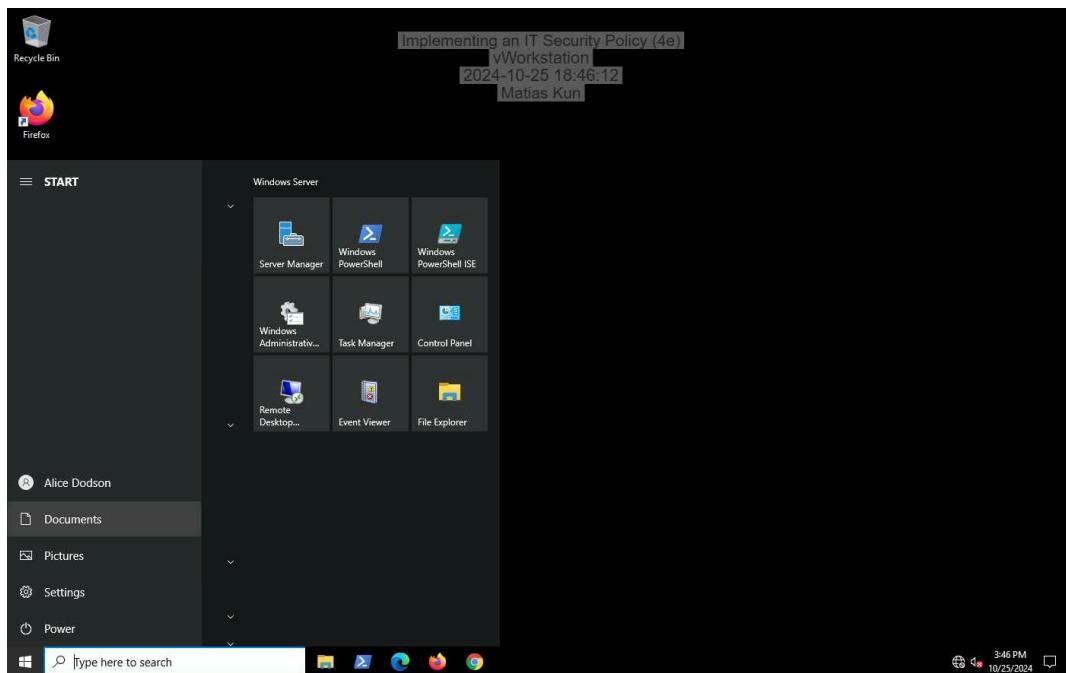
Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

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

Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

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

The screenshot shows the Group Policy Management Editor window. The title bar reads "Group Policy Management Editor" and "Implementing an IT Security Policy (4e) DomainController01". The main pane displays a policy setting titled "Turn off real-time protection" under "Real-time Protection". The setting is named "Matias Kun" and was last modified "2024-10-25 18:56:59". The table shows the following configuration:

Setting	State	Comment
Turn off real-time protection	Disabled	No
Turn on behavior monitoring	Not configured	No
Scan all downloaded files and attachments	Not configured	No
Monitor file and program activity on your computer	Not configured	No
Turn on raw volume write notification	Not configured	No
Turn on process scanning whenever real-time protection is turned off	Not configured	No
Define the maximum size of downloaded files and attachments	Not configured	No
Configure local setting override for turn on behavior monitoring	Not configured	No
Configure local setting override for turning all download...	Not configured	No
Configure local setting override for monitoring file and program activity	Not configured	No
Configure local setting override to turn on real-time protection	Not configured	No
Configure local setting override for scanning for incoming...	Not configured	No
Configure local setting override for monitoring for incoming...	Not configured	No
Configure monitoring for incoming and outgoing file and...	Not configured	No

The notes section indicates that if this policy is enabled, Windows Defender Antivirus will alert users when malware or potentially unwanted software attempts to install itself or run on their computer. It also notes that if disabled, users will be prompted to take actions on malware detections.

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

The screenshot shows the Windows Security app interface. The title bar reads "Windows Security" and "Implementing an IT Security Policy (4e) V:\Workstation 2024-10-25 19:01:58 Matias Kun". The left sidebar shows navigation options: Home, Virus & threat protection (which is selected), Firewall & network protection, App & browser control, Device security, and Protection history. The main pane displays the "Virus & threat protection settings" page. The "Real-time protection" section is managed by an administrator and is currently turned "On". The "Cloud-delivered protection" section is also turned "On". The "Automatic sample submission" section is turned "On". A link to "Submit a sample manually" is present. On the right side, there are links to "Change your privacy settings", "Privacy settings", "Privacy dashboard", and "Privacy Statement".

Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

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.

The screenshot shows the Windows 10 Group Policy Management console. The left navigation pane is collapsed. The main pane displays the 'Account Policies/Password Policy' section under 'Computer Configuration (Enabled)'. It lists several policies with their settings:

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Below this is the 'Account Policies/Account Lockout Policy' section, also under 'Computer Configuration (Enabled)'. It lists:

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

At the bottom, the 'User Configuration (Disabled)' section is shown with the message 'No settings defined.'

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

The screenshot shows the Windows Server Manager dashboard. The left sidebar shows 'Dashboard' and 'AD DS' roles. The main pane displays the 'Group Policy Management' section for the 'DomainController01' domain. The 'Default Domain Policy' is selected. The 'Scope' tab is active, showing the scope is 'securelabondemand.com'. The 'Links' tab shows a link to 'securelabondemand.com'. The 'Security Filtering' tab shows 'Authenticated Users' as the group. The bottom navigation bar shows 'All Servers' with 1 item.

Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

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

The screenshot shows the Microsoft Group Policy Management Editor interface. The title bar reads "MSDomainSecurity2019" and the address bar shows "file:///C:/Users/Administrator/Desktop/MSDomainSecurity2019/MSDomainSecurity2019.gpml". The main content area displays two policy sections:

- Account Policies/Password Policy**:

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
- Account Policies/Account Lockout Policy**:

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

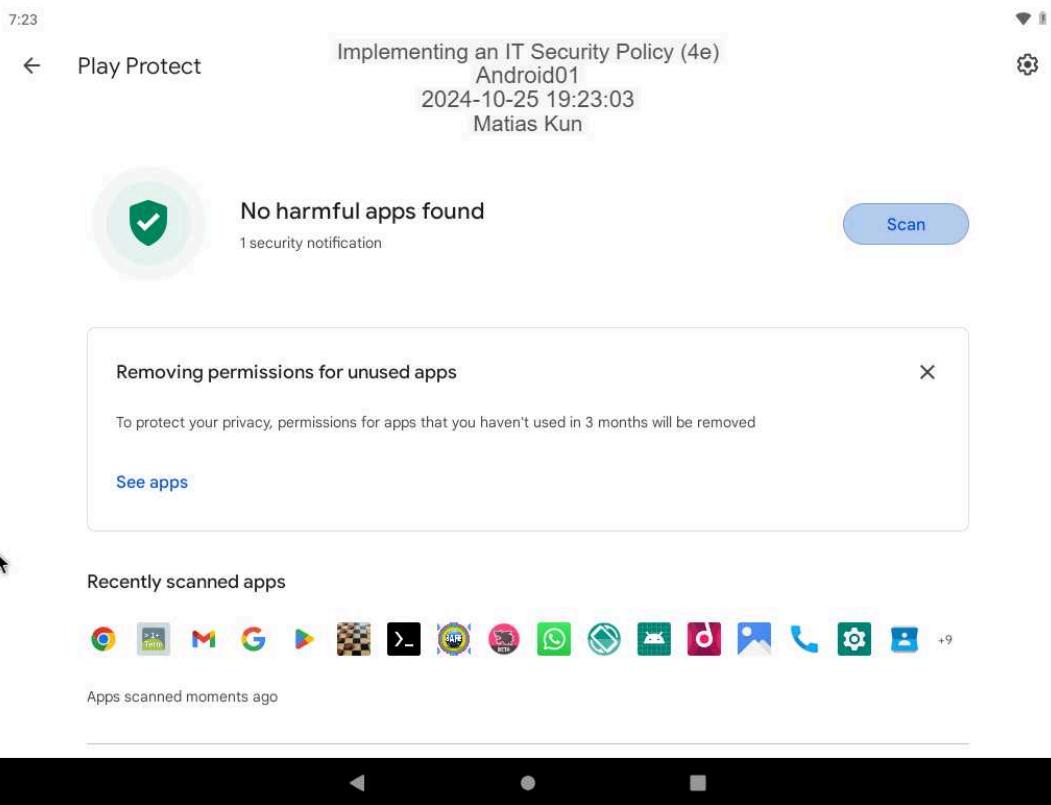
At the bottom, there is a search bar with the placeholder "Type here to search" and a taskbar with various icons.

Part 2: Implement a Mobile Device Security Policy

Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

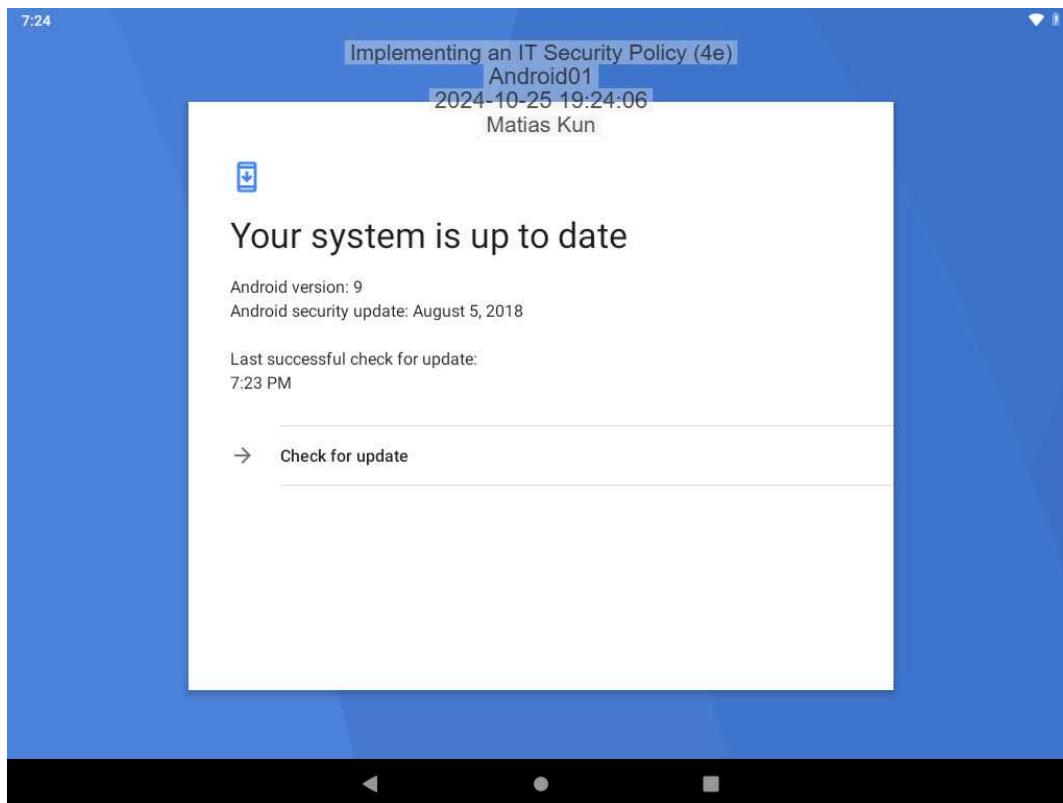
7. Make a screen capture showing the results of the Google Play Protect scan.



Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

11. Make a screen capture showing the updated “last successful check for update” timestamp.



Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

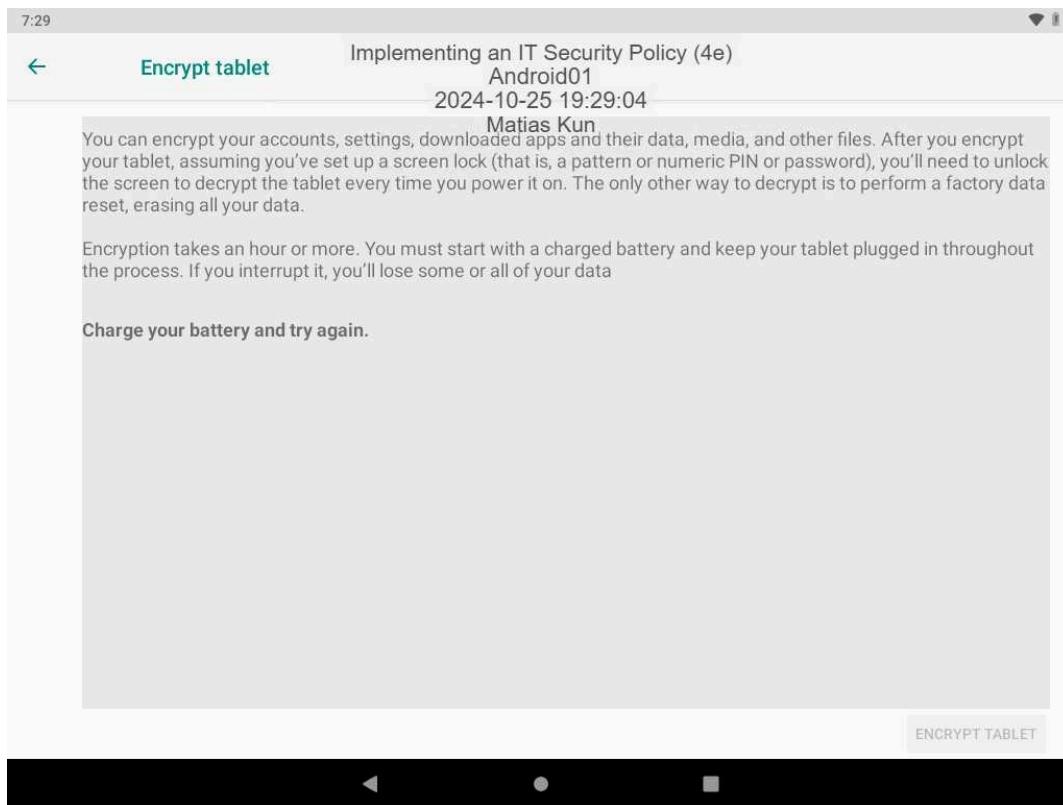
19. Make a screen capture showing the **Android lock screen**.



Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

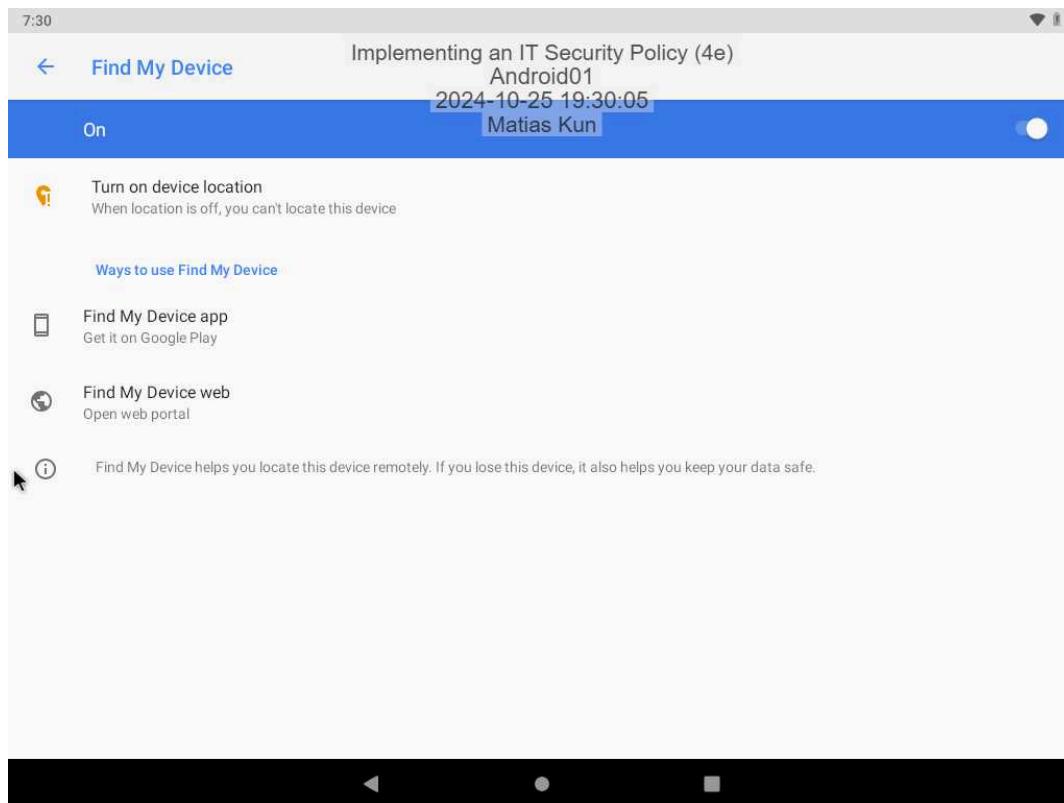
25. Make a screen capture showing the encryption set-up explanation.



Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

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.

Prohibition of Illegal Activities: Most AUPs prohibit illegal actions, such as unethical hacking (black-hat-hacking) and unauthorized access. This is vital for maintaining the organization's integrity, reducing legal risks, and ensuring a secure working environment (University of Tennessee, 2023).

Restricted Use of Company Resources: AUPs often require that company resources, such as networks and equipment, are used exclusively for work-related purposes. This reduces distractions, optimizes bandwidth, and keeps resources available for professional activities (University of Tennessee, 2023).

Cybersecurity Practices: AUPs often include guidelines on password management, data encryption, and other security practices, and they will continually update resources as standards evolve. These requirements prevent data breaches and safeguard sensitive information, thereby reducing vulnerability to cyber threats (University of Tennessee, 2023).

Remote Work and BYOD Policies: As remote work has become more common, AUPs often address device security and network access for remote work. This can include requirements for VPNs and specific security measures to prevent unauthorized access from non-secure networks (University of Tennessee, 2023).

Consequences of Non-Compliance: Many AUPs outline specific consequences for violations, which could include disciplinary action up to termination. This reinforces the policy's importance and accountability standards, protecting both the organization and its employees (University of Tennessee, 2023).

Reference: University of Tennessee. (2023). Understanding Acceptable Use Policies. Retrieved October 25, 2024, from <https://oit.utk.edu/security/learning-library/article-archive/understanding-aups/>

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.

Data Collection and Use: Privacy policies explain what data is collected and how it's used, such as for analytics or user experience improvements (quality assurance). This transparency helps build trust and ensures compliance with data protection laws (PrivacyPolicies, 2023).

Consent for Data Processing: Policies frequently require user consent for data collection and processing, ensuring compliance with privacy laws like GDPR and respecting user control over personal data (PrivacyPolicies, 2023).

Third-Party Data Sharing: Privacy policies often state whether user data is shared with third parties, such as advertising or service partners, so users are aware and can make informed decisions (PrivacyPolicies, 2023).

Security Practices: Privacy policies outline the measures used to safeguard data, such as encryption or restricted access. This assurance supports user confidence in the company's data handling practices (PrivacyPolicies, 2023).

User Data Rights: Many privacy policies inform users of their rights, including access, correction, or deletion of their data, which fosters transparency and supports regulatory compliance (PrivacyPolicies, 2023).

Reference: PrivacyPolicies. (2023). What is a Privacy Policy? Retrieved October 25, 2024, from <https://www.privacypolicies.com/blog/what-is-privacy-policy/>