Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Tuesday, January 28, 2025 at 3:07 PM

Guided Exercises

Part 1: Research Acceptable Use Policies

2. **Write** a **brief summary** of the article. In your summary, focus on the need for an AUP and its key elements.

The need for an AUP exists because human error, neglect, malice, misuse, and abuse are realities that stakeholders in organizations must address to protect themselves, the business, their assets, and their human resources. In the case of this particular article, schools are seeing a growing use of mobile devices, communication, and online media. Schools are obligated to create clear technology use guidelines. AUPs are essential to regulate these devices while utilizing their potential educational benefits and mitigating their risks. Key elements of AUPs are a well-defined scope and purpose, usage guidelines, enforcement, consequences, and cybersecurity protections. An effective AUP will also involve parents, educators, and students working together. Modern policies for schools need to help students navigate the virtual world they are growing up in responsibly while educating students with skills to succeed in the digital world of their future.

Part 2: Design an Acceptable Use Policy

3. **Design** an AUP for this fictional credit union, using the online example of the AUP as a template. Your policy does not need to be exhaustive, but it should outline the key components of an AUP and provide policy statements that address the above requirements. You may want to create your policy using word processing software on your local computer and then copy and paste the text into the deliverable field.

Acceptable Use Policy
This Acceptable Use Policy (AUP) establishes guidelines for the acceptable use of the credit union's IT resources. It supports compliance with the Gramm-Leach-Bliley Act (GLBA) and IT security best practices. All employees at any branches owned and/ or operated by the credit union, contractors, and affiliates must follow this policy when accessing and using the credit union's network and IT resources.

Brief & Purpose

The purpose of this AUP is to ensure compliance with law and IT security best practices, maintain reliability, and protect the privacy of the credit union's IT resources, employees, and users' data.

Scope
This policy applies to all users who access the credit union's IT resources, including employees, contractors, visitors, and external partners.

Acceptable Use
IT resources must be used solely for business purposes related to the credit union.
Employees must follow security protocols and protect customer information per GLBA requirements.
Employees must complete annual security awareness training and acknowledge this policy.

Prohibited Use
Personal use of IT assets, including email, internet, and computing devices, is strictly prohibited.
Accessing, transmitting, or storing unauthorized, offensive, illegal, or inappropriate content is forbidden.
Employees must not attempt to bypass security controls or content filtering measures.

System and Network Activities
The credit union will monitor and control internet and network activity through content filtering.
Users must not introduce or attempt to introduce malicious or any intentionally harmful software into the network.
Employees must not attempt to gain unauthorized access to any IT system.

Email and Communication Activities
The credit union's email system will be used only for business-related communication.
Approved IT personnel will implement Email security controls to prevent phishing, spam, and unauthorized access.
Approved IT personnel will implement monitoring controls to monitor the use of the email system.
Employees must not email sensitive information without authorization.

Confidentiality
Employees must protect confidential information and maintain compliance with the Gramm-Leach-Bliley Act (GLBA).
Sensitive data, including customer information, must be accessed only for authorized business purposes.

Enforcement
Employees found violating this policy may face disciplinary action, up to and including termination of employment and potential legal consequences.

Review and Revision
The credit union stakeholders and IT department will review this AUP annually and update it as needed to comply with regulatory and operational changes.

Agreement
By accessing and using the credit union's IT resources, you acknowledge and agree to comply with this Acceptable Use Policy.

Challenge Exercise

Select an industry other than banking. For example, you could choose manufacturing, higher education, or utilities.

Healthcare Industry

Create a list of unique attributes of the business in your chosen industry.

HIPAA - Health Insurance Portability and Accountability Act

State laws protecting patient data protection

Protected Health Information (PHI)

Access based on roles such as doctors, nurses, technicians, and administrators

Regular audits and monitoring for access logs

Smart internet-connected medical devices introduce security risks.

Healthcare is a prime target for ransomware, phishing, and insider threats.

Emergency rooms, Intensive Care Units, and surgical operations require uninterrupted IT availability.

IT downtime can result in loss of life or severe health consequences.

Instead of creating an AUP, **write** a formal letter to the company's CEO and board to explain the need for an AUP and your suggestions on the content of that policy.

Dear Healthcare CEO and Members of the Board,

The healthcare industry faces unique cybersecurity threats that require regulatory compliance and endanger patient safety. To mitigate these unique risks to an acceptable level and align policies with HIPAA and state laws, we must implement an Acceptable Use Policy (AUP) for IT resource security. Given the sensitivity of Protected Health Information (PHI) and the healthcare industry's adoption of innovative medical devices, role-based access controls, and real-time data availability, an AUP is critical to ensure our IT infrastructure's secure and ethical use. I have included the following suggestions on the content in an acceptable use policy.

To protect PHI, all personnel must adhere to HIPAA, state laws, and internal security protocols. System access should be restricted to doctors, nurses, technicians, and administrators based on job function, implementing least privilege access. Authorized IT personnel must conduct routine access audits and ensure compliance. Employees must complete mandatory cybersecurity training. IoT medical devices must maintain a secure and updated status by authorized IT personnel against cyber threats. Emergency and critical care units must not accept IT downtown; this will ensure patient safety and maintain uninterrupted operations. Implement a structured cyber incident response process and plan to address security concerns.

Leadership should prioritize this policy to enhance security, maintain compliance, and protect patient lives. I welcome the opportunity to discuss implementation strategies.

Sincerely,
Bradley Adams