# *IT Security (420-F30-HR)*

# *Lab 11 – Security Policy – Acceptable Use Policy, Training*

Date assigned: Tuesday, April 8

Date Due: Tuesday, April 8, 3:30PM (before end of class)

**Objectives:**

Learn:

1. Standard Employee training
2. Acceptable Use Policy concerns

# Employee Training

Review the Amazon employee training. [Here](https://learnsecurity.amazon.com/), takes about 15 minutes.

Follow the eLearning path, then take the test at the end to get certified.

The goal is to see an example of a company’s employee training.

Collect information from each of the sections and fill in the table.

|  |  |
| --- | --- |
| Scenario | Response |
| Received email with links in it. | Look at the FROM  Look for spelling or grammar errors |
| Co-worker wants to send business details to their personal email. | Let them know they can’t share business plans outside of company email addresses. |
| Valid reason for allowing a co-worker to use your badge or credentials. | No valid reason |
| What to do with whiteboards or printed materials after the meeting is done? | Wipe them |
| If you need software that isn’t on the approved list. | Contact security team |
| News reporter asks for launch date for new service or product | Don’t share confidential info. |
| Left your laptop in your car on the front seats. | Go get your laptop, or hide it in the car |
| Asked to register/join a mailing list. | Contact security team |
| Request from a co-worker comes in from an external chat app. | Don’t use 3rd party apps |
| Call received from unknown number | Don’t pick up, report the number |
| What’s the reward for completing the test successfully | My certificate! |

Provide a screen shot of your Certificate of Completion:

A black background with white text

Description automatically generated

Assess. Do you think this training is effective in teaching employees about IT security? Why or why not? Any suggestions for improvement?

Not effective at all, you can skip to the test at any time. Design is nice and captivating though.

Why do you think that a lean, time-is-money, company like Amazon wants every employee to go through this training?

Because its super easy to get through and a made-up certificate with no value

# Use Case - College

The Heritage Acceptable Use Policy can be found [here](https://cdn.cegep-heritage.qc.ca/documents/PDF/policies_and_regulations/policies/Policy-23-Use-of-Electronic-Networks.pdf?1591134154).

1. Is the college allowed to track your activity on college network and resources? Provide the source information to backup your answer.

Yes, they are allowed.

"The departmental electronic networks are routinely monitored for operational reasons... necessary to assess system or network performance, protect College resources, and ensure compliance with College policies."

1. If legally requested, does the college have to provide your usage data, such as web sites visited, email, etc.? Provide the source information to backup your answer.

Yes, they have to provide if requested.

The College could find itself under legal obligation to provide access to these records.

1. Identify which section you are in violation of for the following activities:

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Activity | Section | Applicable Rule Violation |
| 1 | You setup a gambling server running on one of the lab PCs, you take a 10% cut of the business generated | 5.3 | Using the internet … for illegal gambling |
| 2 | Using Heritage email to pass around an open-source game | 5.2 | Adding or downloading computer games |
| 3 | Posting a bomb threat on a college message board | 5.3 | Sending electronic messages… that cause people to fear for their safety |
| 4 | Reading someone else’s email once they step out of the room | 5.3 | Privacy infractions such as reading someone else’s email |

1. Roles and responsibilities. Identify who is responsible for the following, include your reference:

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Activity | Section | Who |
| 1 | Employee leaves college. Terminate access to college data resources. | 6.2.2 | Senior Managers |
| 2 | Periodically assess the need to update the policy | 6.2.3 | Senior Management Team |
| 3 | Investigate report of unlawful activity by user | 6.2.1 | Coordinator of Computer Services |

1. Identify sections that cover the indicated:

|  |  |  |
| --- | --- | --- |
| # | Activity | Section(s) |
| 1 | Who the policy applies to (users) | Article 4 – Application |
| 2 | What you’re allowed to do | 5.1 – Acceptable Activity |
| 3 | What you’re not allowed to do | 5.2 – Unacceptable Activity & 5.3 – Unlawful Activity |
| 4 | Roles and Responsibilities | Article 6 |
| 5 | Penalties | Article 7 – Disciplinary Measures |

1. Were any of these policy rules surprising to you? If so, what was surprising and why?

Yes, I was surprised that even reading someone else’s email without permission is explicitly listed as an unlawful activity. The policy rightly treats it as a privacy breach.

# Use Case - Business

A film executive returns to work after being at a tradeshow most of the weekend. On Monday morning, he receives a first-class, signature-required package addressed to himself. The letter is from a production company he met with at the tradeshow – it’s on official letterhead and the names are of the people he met. There’s a USB drive with the production company’s logo on it that supposedly has a few trailers on it for the executive to watch.

If you’re the executive, what do you do?

In real life, this executive plugged the USB drive into his machine. The firmware of the USB stick then automatically installed drivers without him clicking on anything, releasing a virus that led to one of the largest media piracy events in U.S. history. Weeks later, movies that were still in the theatres were now also on the internet, costing the film studio billions of dollars in potential sales.

## Reference [here](https://www.comptia.org/blog/security-awareness-training-corporate-acceptable-use-policy)

1. What is an Acceptable Use Policy? Explain the purpose of it and how it could have addressed this use case.

An Acceptable Use Policy (AUP) is a set of rules and guidelines that outline how users are permitted to use an organization’s IT systems, networks, and devices. The purpose of an AUP is to protect both the user and the organization from misuse, legal liabilities, data breaches, or security threats.

In the USB case, if the company had a strong AUP that included rules about the handling of external devices, the executive would’ve been instructed to never plug in unknown USB drives, even if they appear legitimate. Instead, the device should have been scanned or handled by IT security staff. This could have prevented the malware infection and subsequent massive piracy event.

1. Write rules that you’d put into an Acceptable Use Policy document that covers USB drives, BYOD, company network use and external networks that addresses:

* How to handle new USB devices

All USB drives from external sources must be scanned by the IT department before use.

Plugging in personal or unknown USB devices is strictly prohibited unless approved and scanned.

If a USB is received unexpectedly or from an unverified source, report it immediately to IT Security.

* What types of devices can employees use on the corporate network? If employees and guests can connect their own devices to the corporate network, are they any restrictions about what they can do on the network?

Only company-issued devices or personally owned devices registered with IT are permitted on the internal network.

All devices must run up-to-date antivirus software and comply with the company’s security configurations.

Unauthorized devices will be blocked or removed from the network.

* Can guests use the network or Wi-Fi? Is there a guest network for devices not issued by the company? Can employees connect company-owned devices to other networks at all?

Guests must use the designated Guest Wi-Fi. Access to internal company resources is strictly forbidden on guest networks.

Company-owned devices must not connect to guest networks to avoid data leakage.

* What types of networks can company-owned devices be connected to? (For example, a private home network, a private network operated by another company or a public coffee shop network.)

Company-owned devices may only connect to:

Secure home networks (if remote work is authorized).

Private business networks (with prior IT approval).

Public networks (e.g., coffee shops, airports) should only be used with VPN protection and limited access to sensitive data.

Company data must not be accessed or transferred on public or unencrypted networks.

Look up best practices and provide references for how you came up with the rule.

<https://www.cisa.gov/sites/default/files/publications/CISA_Insights_Remote-Work_Tips_0.pdf>

<https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy>

# Policy

In general, what’s the benefit of studying organization security policies?

Studying organization security policies helps employees understand their responsibilities and boundaries when using company resources. It:

* Promotes a security-first mindset, reducing risk of breaches.
* Ensures compliance with laws and regulations (e.g., privacy laws).
* Protects sensitive data and systems from intentional or accidental misuse.
* Clarifies what’s acceptable and what’s not, so people don’t break the rules unintentionally.
* Supports a consistent organizational culture around IT use and ethics.

Picture yourself in a boat on a river. You are an executive of a medium-sized IT company pondering about security policies. You currently have none. You’re on vacation, but when you get back, you’re interested in designing and implementing policies.

Define and design policies that an employee will be subject to from recruitment, onboarding, day to day life, and final off-boarding.

Provide a list of policies. For each:

|  |  |  |
| --- | --- | --- |
| Name of Policy | When and who policy is applied | Purpose, short description (2-3 sentence) |
| HR - Hiring | At recruitment, applies to hiring managers and HR | Ensures background checks and reference verification are done to assess risk before granting access to systems. |
| HR - Onboarding | Applies to new employees on their first day | Introduces new hires to IT policies, acceptable use, and gives them secure credentials. Includes signing AUP agreement. |
| AUP (Acceptable Use Policy) | Applies to all users during employment | Defines acceptable and unacceptable behavior when using company devices, email, internet, and networks. |
| IT Operational Policies | Ongoing, applies to all employees and IT staff | Covers things like password policies, software installation, device use, remote access, incident reporting, and regular updates. |
| HR - Offboarding | Final day of work, applies to HR and IT | Ensures access is revoked, devices returned, and exit interview covers confidentiality and data protection obligations. |

**Marking Scheme**

|  |  |
| --- | --- |
|  | **Out of** |
|  |  |
| **Part A: Employee Training** |  |
| Table entries | 12 |
| Certificate of Completion | 2 |
| Assessment | 4 |
|  |  |
| **Part B: College Acceptable Use Policy** |  |
| 1 | 2 |
| 2 | 2 |
| 3 – Table | 8 |
| 4 - Roles | 6 |
| 5 - Sections | 5 |
|  |  |
| **Part C: Business Acceptable Use Policy** |  |
| 1 – AUP definition | 4 |
| 2 - Rules |  |
| USB | 4 |
| Devices on corp network | 4 |
| Using company devices on other networks | 4 |
|  |  |
| **Part D: General Policy** |  |
| 1 – why? | 4 |
| 2 - table | 10 |
|  |  |
| Handed in properly | 4 |