The Acceptable Use Policy

Joseph Foley

Old Dominion University

Cybersecurity Strategy and Policy

Professor Teresa Duvall

September 15, 2024

The cybersecurity policy that I have selected is the acceptable use policy. I chose this policy because its crucial in order to have guidelines and rules for a company. I believe this policy is needed to help organizations have a clear understanding on their resources to safeguard legal, operational, and security risks. This is done because it outlines the data an organization has and institutes an agreement to protect these resources.

A general overview of the acceptable use policy is that it's used to address allowed or prohibited permissions, and it applies consequences through monitoring. It sets who and what can be done to actions that are done on an organizations information system. This is important because anyone accessing any website can be a major security concern. This system can also deny access to certain websites or media to avoid this from taking place. Another thing the acceptable use policy addresses is disciplinary action to people if the agreements are broken, as well as being able to monitor all traffic coming in from employees while they are on the data system. These general principles are instituted in order to make sure the acceptable use policy is able to protect an organization and limit operational risks.

The acceptable use policy was developed to do many things to organizations such as protecting system infatuation, protecting data integrity, and maintaining general productivity. To protect these systems contracts are typically enforced as soon as employment begins to make sure they understand the rules of the contract they're agreeing to. To apply the acceptable use policy these terms and conditions need to thoroughly implicated and communicated within an organization.

It is applied in many ways in organizations internationally and is used to integrate new employees or third parties. This is done to ensure the integrity of the employee as well as that they understand the agreement that's presented in the acceptable use policy. To apply the acceptable use policy there are many things that can be done such as awareness training, configuring access controls, monitoring data, and taking response to actions.

The policy fits within both national and international cybersecurity policies and is often associated into many frameworks. The National Institute of standards and Technology or NIST cybersecurity framework for example focuses on how it protects functionality to make sure data is secure. This helps encourage and develop strong policies that will help mitigate potential risks. Acceptable use policy will typically align with different frameworks because they meet the same requirements for regulating data security.

Overall, the usage of acceptable use policies is crucial in order to keep data secure, safeguard the company's resources, and to provide legal compliance to frameworks. It is

helpful because it is able to ensure that the standards are always upheld, or certain disciplinary action is taken. These procedures are necessary in order to make sure an organizations information systems are secure. When other cybersecurity frameworks align with the acceptable use policy, they are able to enhance the security by setting clear expectations.

Sources Cited

Lichtenstein, S., & Swatman, P. M. (1997). Internet acceptable usage policy for organizations. *Information Management & Computer Security*, *5*(5), 182–190. https://doi.org/10.1108/09685229710367726

Flack, G. P., Kritzinger, E., & Loock, M. (2021). Improving Compliance with the Acceptable Usage Policy. In *Lecture notes in networks and systems* (pp. 621–635). https://doi.org/10.1007/978-3-030-77448-6_61

Stephen, B., & Petropoulakis, L. (2007). The design and implementation of an agent-based framework for acceptable usage policy monitoring and enforcement. *Journal of Network and Computer Applications*, *30*(2), 445–465. https://doi.org/10.1016/j.jnca.2006.06.004