Acceptable Use Policy

 [Author Name]

[Institutional Affiliation(s)]

Acceptable Use Policy

An acceptable use policy (AUP) is a set of rules and regulations that are applied by the owner of any website or network to pose restrictions on the ways through which websites or networks may be used. The owner or administrator also provides guidelines on how the network or websites should be used. AUP is an integral part of the information security policies (O'Byrne, 2019). AUP documents are not only limited to the information security field as this policy is also implemented in educational institutes, businesses, and any other organizations. A security breach is one of the major issues that is faced by many organizations. Although, these issues are highlighted regularly yet still, many organizations do not have the required knowledge of how to avoid a security breach. In most cases, the reason for a security breach is the lack of policies or loopholes in the contracts that organizations, networks, and institutes typically ask new employees or users to sign. To avoid this issue, it is recommended to use an acceptable use policy as this policy is not meant to snoop on others but it the policy that facilitates in protecting business assets.

Modern life spins around technology and it has become an indispensable part of our life. Regardless of age, people are using the internet every day. Due to this reason I have decided to focus on the AUP policy that governs internet usage. AUP regarding the usage of the internet does not only include a website or network information that can be accessed by the end-users, but it also includes information that is prohibited to access. The AUP will not only help in protecting an organization from any illegal actions and damages but it will also protect the people working within an organization as well (Stewart, 2000). The foundation of information security is laid on three principles. These three principles are confidentiality, availability, and integrity. AUP helps a lot in ensuring that all three principles are followed and implemented in any organization by limiting the accessibility of the confidential information. The AUP contains a clause that allows only authorized people to access confidential information while preventing unauthorized people from accessing confidential information. Additionally, the policy requires that even the authorized people must authenticate themselves before accessing the information. This will help a lot in securing the information as if any information is disclosed, then the employee is held responsible and the organization can take legal action against them. This policy is not limited to confidential information but can be implemented on the internet usage of the whole organization. For instance, if employees are using the internet for accessing or contacting competitors’ sites or entertainment purposes rather than doing an organization’s work, then they must be held accountable according to acceptable use policy. On the other hand, an organization is not allowed to spy on employees’ emails as this is also a kind of privacy breach and employees can also take legal action against the company. Thus, using this policy will not only benefit the company but the employees as well.

The acceptable use policy for internet users should not be limited to entertainment sites usage or accessing competitors only but it should be used to control cyberbullying and creating or distributing unlawful content. The policy can further be improved by introducing the rules against cybercrime as well. This will help in mitigating any illegal actions that can damage a company’s reputation. Also, this will help in saving employee’s personal information from leaking.

The AUP for internet usage can be implemented in an organization by providing the employees with two copies. One copy will be with them while the other copy must be submitted back to the organization. All the details of the policy must be communicated to the employees so that they can understand the terms and conditions before signing the contract. Furthermore, the policy must be created by incorporating the employees' needs while also considering their privacy and security as well. The companies must ensure that all the employees are aware of the policy to avoid any issue. The implementation of the AUP policy will act as a counter-strategy to mitigate the risk of exposure of confidential information and inappropriate use of the internet (Safa & Furnell, 2016).

Organizations can utilize several techniques to spread awareness of their internet usage policies. It is relatively easy for a company to provide a contract to the newly hired employees so that they can be aware of the policies. However, it is a bit difficult for a company to spread awareness regarding its internet usage policies to the public. A company can be aware of the public by using brochures and displaying posters in public places so that company staff and the public can see them. The companies must pin the brochure on their websites so that customers and employees must be aware of their limitations while using internet services. A company can also conduct sessions and seminars to the employee awareness of the terms and conditions regarding internet usage. The sessions are very helpful as during sessions, the employees can share their concerns and ambiguities that can be solved instantly (Gaskin, 1998). The sessions can also be aware of the employees regarding the repercussions that may arise if they violate any of the company’s policies. Additionally, the employees will also be able to know about their rights and access as well. Thus, every company must implement the AUP for internet usage to ensure confidentiality, availability, and integrity.

**References**

Gaskin, J. E. (1998). Internet acceptable usage policies. *Information Systems Management*, *15*(2), 20-25.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70-82.

O'Byrne, W. I. (2019). Acceptable Use Policies. *The International Encyclopedia of Media Literacy*, 1-6.

Stewart, F. (2000). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Information Systems Security*, *9*(3), 1-7.