Acceptable use policy review and discussion case study examples

Education, University

An acceptable use policy (AUP) is an essential document for several types of organizations, including businesses, educational institutions, and service providers, that lays out the rules applied when accessing the owner’s network. While AUPs are often used to describe the general employee code of conduct when engaging in discussions online, they are usually a part of information security policies, which indicate how employees may access confidential information and what consequences will be enforced in case the policies are breached.

The AUP developed by Clemson University offers clear guidelines on employee conduct when engaging with the computing systems provided on the campus. The policy aims to improve the protection of information technology resources and data supplied and used by Clemson University (2009) because the availability of desktop computers increased the responsibility of individual employees when safeguarding confidential information. In addition to the protection of privacy and digital resources measures outlined in the AUP, Clemson University (2009) mentions that several Federal and State statutes may apply to the information kept in the University computer systems.

In terms of confidentiality, the AUP complements other policies, such as the Username and Password Policy and the Strong Password Guidelines, which provide instructions for safeguarding personal information and minimizing intrusion liabilities. Although physical safeguards are not discussed explicitly, it is possible that several measures, such as authorization cards to access server rooms, are probably implemented to protect confidential data or allow access only to employees responsible for installing service packs and

patches. The University responsibilities include implementing reasonable protection against hardware failure, sabotage, theft, or human errors.

In order to increase confidentiality, integrity is expected from employees. However, without clear rules, organizations are at risk because they will lack loss mitigation strategies and assume legal responsibility for their employees' actions. The Clemson University AUP bans using their network for personal gain or illegal activities, but it also provides instructions of how employees can implement physical safeguards themselves to avoid social engineering attacks and granting unauthorized access to third parties. Compliance, and thus employee integrity, is improved by introducing consequences for breaking the rules.

Finally, the policy discusses how Clemson University combines the availability of information technology with various safeguards in place to protect confidential information and system functions. Although Clemson University does not reveal its position on social media during work hours, it is most likely approved as long as employees do not abuse social media in a way that would violate several terms outlined in the policy, such as by disclosing confidential information or revealing access information to secured systems. However, it is important to mention that Clemson University monitors user activity to prevent system misuse, so surfing the internet may be restricted in case employees visit sites or social network pages that are associated with high security risks, such as sites with adult content or spam bots on social networks.

In most cases, the rules and regulations in Clemson University's AUP define clear expectations from their staff, which is important to avoid

misinterpretation and minimize losses and risks. However, a lot of points discussed in the AUP are general, and the policy lacks clear emergency response descriptions and disciplinary actions. For example, the complementary Investigations Policy only defines the responsible parties in investigating suspicious activities without clarifying the response requirements for specific types of policy breaches (Clemson University, 2013). Another example is a lack of systematic disciplinary action descriptions in the policy. The organization describes the severity of the breach and previous instances of disciplinary actions determine the severity of the punishment (Clemson University, 2009). However, between a short suspension and losing the job, there is a lot of room for interpretation and bias, so it would be fair to list disciplinary actions transparently in the policy. Clemson University AUP should also be more explicit in terms of employee authorizations. For example, it is reasonable to expect that system administrators will have fewer restrictions in accessing confidential information and local systems. However, according to Samuelle (2008), access control policies need to be further elaborated because they define which job positions have access to system files and confidential information. For example, job rotation is a frequent strategy implemented to ensure employees do not maintain the same level of power and responsibility, which may lead to misuse of the security access they are granted. Implementing those policies would improve the confidentiality and integrity at the workplace.

Finally, the structure of the document is important to improve readability and comprehension. For example, the policy uses the “ General Guidelines”

subheading to list all rules enforced by the AUP. The e-mail policy, loss mitigation, back-up protocols, and individual responsibility are all discussed under the same subheading, which leads to lack of details in each case and lack of structure. The AUP should be organized to allow employees to use it as a reference when necessary rather than needing to read the entire document when looking for a specific piece of information.

Although several improvements are still possible, the policy does cover loss mitigation, risk prevention, and legal liabilities. For example, employees are explicitly instructed to never reveal their username or passwords, but the organization also provides a reference to their guidelines on choosing strong passwords to minimize the risk of unauthorized access (Clemson University, 2009). The policy also mentions that all employees are required to inspect their hardware and software to prevent implementing devices or programs that provide unauthorized access to the network by third parties.

If an information security threat is detected, the employees are instructed to report the issue to Departmental TPSs, College Consultants, or to the IT Support team (Clemson University, 2009). However, further clarification of potential scenarios is required. For example, there are no responses defined in case a natural disaster occurs. Furthermore, the responses to possible mySQL, cross-site scripting attacks, and similar threats are not mentioned. A good policy should assess all possible risks and develop general plans of action in those scenarios.

In order to increase the awareness of AUP and several other security-related policies within the organization, the best method is to maintain a constant communication between the human resources department and employees

from other departments. The familiarization with company policies should not begin too early, such as during job interviews, because revealing the AUP without signing a non-disclosure agreement may lead to revealing the safeguards implemented and allow unauthorized individuals easier access with appropriate exploits. When the potential employees are offered a job, they should be instructed to sign the AUP in addition to the job contract (SpectorSoft, 2013).

Finally, orientation briefings may be beneficial to new employees to provide them with everything they need to know about the company policies. In order to increase compliance rates, the company can include the possible legal implications for illegal actions beyond organizational sanctions. Such instances include violations of State and Federal laws, which may lead to legal trials and incarceration in addition to losing the workplace.

References

Clemson University. (2009). Acceptable use policy for employees. Retrieved from http://www. clemson. edu/ccit/about/policies/accept_use_employee. html

Clemson University. (2013). Investigation policy. Retrieved from http://www. clemson. edu/ ccit/about/policies/investigations_policy. html

Samuelle, T. J. (2008). Mike Meyers' CompTIA Security+ certification passport. New York, NY: McGraw-Hill, Inc.

SpectorSoft. (2013). Bring your acceptable use policy up to 2013 standards. Retrieved from http://downloads. spectorsoft. com/resources/WhitePapers/ WP_InternetAcceptableUsePolicy. pdf