Acceptable use policy critical thinkings example

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Purpose of an acceptable use policy

An acceptable use policy is a policy that a user should agree to follow so that they are allowed to use a computer resource. Many organizations require that employees and other computer resource users sign acceptable use policy before they start use the computer resources. They provide the etiquette in which computer resources will be used in the network. AUP is supposed to define what needs to be followed in the use of computers. They will define the limits that each group has, and the privacy that is to be followed. AUP is meant to protect group members from getting illegal content like pornography, offensive language, and influences which are regarded to be questionable. The use of the AUP in a fire department will define the requirements and the procedures that should be followed in order to access the network.

The AUP will also define the boundaries in which the users are allowed to

access in the network. It is important to understand the procedures that one should follow while using the resources of the computer network in the fire department. With the advent of computer security breaches and the security issues of computer networks, the policy is meant to protect the other users from attacks online. With the AUP, there is a requirement that there is ethical use of the computer network of the fire department. This will ensure that there is no harassment, violation of security policy, and wrong use of data that entails the fire department. In the fire department, there will be the laying down of rules that will be followed in that fire department. This will guide in the use of the computer network in the fire department so that the security of the department is assured.

Another purpose of the acceptable use policy in the fire department is to make sure that the users in the fire department respect the computer network of the fire department. This will ensure that the users use computer resources and the network in a respectable manner. This will enable the use of the computers with respect to the policies that have been laid down by the fire department. It will enhance security of the network in the long run. The AUP for the fire department will also protect the use of network bandwidth inappropriately. There will be ways and limits through which the bandwidths will be used to protect the network. This will also ensure that applications that are not used in the department might be limited in their access and use of the bandwidth or may be blocked altogether if they appear to misuse the network bandwidth.

Audience being addressed

The audiences that are being addressed are the users of the computer network in the fire department. This will include the clerks who use the desktop computers in the fire department. This is because all officials who work in the fire department are required to follow some rules and policies that have been set up by the fire department. This will ensure that the users have knowledge of how they should be able to use the network resources of the company.

Another group of audience that the policy is to address is the management. The managers are required to know the policy so that they are able to enforce the policy. Any violation should be corrected and the managers are the people who are required to help the fire department enforce the AUP.

Another audience is the administrators who will manage the network. These are the information technology staff that will be tasked with ensuring that the AUP has been implemented in the company. They will ensure that the resource is used as per AUP. They will monitor the network to check if there are violations of any part of AUP. They should, therefore, understand the AUP.

Privacy expectations

There are privacy expectations that are required from users. They are indicated in the acceptable use policy. One of the privacy concerns is that users will not be allowed to sniff the network using sniffer tools. This is a privacy concern that is expected to be included in the UAP. Sniffing tools are known to disrupt the normal operations of the network. This will also affect the privacy of other network users.

Another privacy expectation is that users will not be allowed to surf sites which are suspicious. In the use of the internet from the premises of the fire department, users will not be allowed to surf sites which are known to affect the integrity of the whole system.

Users will also be required to safeguard their security credentials like the password and username. This is to protect unwanted intrusions to the network. The users should use the network access privileges alone. They should also protect these credentials in safe places that will not be easily accessible. Users are required to change their passwords frequently.

Requirements of the municipal leadership

The municipal leadership is required to come up with the policy. They are required to ensure that the network resource has been protected from careless use. This will protect the users from misusing the network. They will come up with the AUP and ensure that it is updated regularly according to the technology trends that are experienced every day. The leadership will also ensure that privileges have been set by the administrators and that all the staff follows these privileges.

The municipal leadership will also ensure that there is sufficient training for the employees so that they understand the requirements of the policy. This way, they will be able to follow the procedures and laws that have been set by the policy.

Responsibility of the municipal employees

The municipal employees will be required to use the computer resources, especially the network in a responsible manner. The employees will be

required to protect their access rights to the system. This will ensure that the security of the network lie with them. They will be required to change their passwords regularly.

The municipal employees will also be required to ensure that the computers and network resources they use have security tools that will protect their computers from attacks. They will ensure that the computers are safe from attacks. They are required to ensure that the security status of the desktop computers is optimized. They should use secure administrator password and ensure that they make use of the latest security updates concerning computer networks. All users who are subscribed to the network will be responsible for all the connections within the municipal offices. They will ensure that the connections are safe and follow the latest security standards.

Municipal users will remain subject to laws that are defined outside the municipal fire department. They will be required to follow network policies that are defined by the federal government. The violations of these policies will undergo prosecutions that are stated in the local government or national government. They will be required to go through these laws and understand the requirements that are to follow. The fire department will reserve the right to investigate the violations that have been claimed by the authority undertaking the investigations.

It is the responsibility of employees to ensure that unwanted applications are not installed ion the network. They will only install applications which are allowed in the network. This will ensure that only safe applications will be allowed in the network. This will also ensure that the bandwidth of the

municipal is used fairly. There are some applications which consume a lot of bandwidth.

Municipal employees will be responsible for all connections that they authorize. The users will be held accountable for any violations that are undertaken in their computers or network connections.

Disciplinary action

If any computer network user violates the stipulated acceptable use policy, there are disciplinary actions that will be laid down for the users. One of the disciplinary measures that will be taken for anyone who violates the network is disconnection of the computer they use from the network. Depending on the degree of the violation, the user may be disconnected for long periods of time.

Users may also get capping of network usage. This is if the network users overuse the bandwidth of the network and the resources that they have been assigned. The users will be terminated from the network resource without notice if they violate the network.

References

AT&T. (2008, October 15). AT&T Acceptable Use Policy. Retrieved February 8, 2014, from AT&T: http://www. corp. att. com/aup/

Mitchell, B. (2014). Acceptable Use Policy - AUP. Retrieved February 8, 2014, from About: http://compnetworking. about. com/od/filetransferprotocol/a/aup_use_policy. htm

SANS Institute. (2006). InfoSec Acceptable Use Policy. Retrieved February 8, 2014, from SANS: http://www. sans.

org/security-resources/policies/Acceptable_Use_Policy. pdf

Worcester Polytechnic Institute. (2008, August 19). Acceptable Use Policy (AUP). Retrieved February 8, 2014, from Worcester Polytechnic Institute: http://www. wpi. edu/offices/policies/aup. html? shortURL= aup&redirector= plus. wpi. edu