Ryan Krage
P4

P4 – Security Policies

Security policies are a set of rules that users agree to when using IT systems to keep the system secure. They are rules and not guidelines, and cover a specific area, such as acceptable use or security.

Most schools and workplaces have IT policies, as well as some places with public computers (libraries, internet cafes). The more critical the system is, the stricter the policies will be. Policies are designed to prevent damage to systems – accidental or otherwise. Generally, they cover vulnerable areas of the system, and instruct users not to anything that could damage them. For example, schools will not allow students and staff to misuse computer resources, such as network bandwidth or printers. A more important system may have stricter policies in place, such as not allowing systems to be used without permission to ensure they are not misused.

Policies will also have more specific rules, such as not allowing certain activities on the computers (gaming, watching non work-related videos, etc.). Many policies will also have a section on what can be done with the hardware – in some places everything must go through the IT or HR department and users are not allowed to do anything with the hardware (such as swapping out a broken keyboard), and some places are less strict, allowing users to bring their own peripherals. For systems that contain critical information, they may not even be allowed to use USB sticks, as it is possible they could contain malicious code.

The network of any system will be covered in its policies. Most will cover some basic do’s and don’ts, such as not using bandwidth without good reason, or not sending spam email.

Another thing the IT policy will address is the user’s responsibilities – these range from not sharing confidential data and credentials, to ensuring they use a strong password and regularly changing it.

Often, there will be multiple policies for each area of a system, and a general one that refers to the others. Areas that can be covered include:

- Networking
- Acceptable use
- Wireless communication
- Remote connections
- BYOD
- Accidental damage/loss
- Passwords
- Email
- Disaster recovery

A policy can be as specific as the system it covers, so there may be many, many policies for a large organization. Usually, users will only see one or two, and it is administrators and IT technicians that deal with more specialized systems.