A Laptop Security Policy

WinEncrypt

What is a laptop security policy?

Laptop security policy is a document that states in writing the rules and practices to be conformed to at all times by the employees of an organization in order to ensure the safety of laptops issued to them and the data stored in the machines. Laptop security policy is ideally framed by IT professionals of the organization and signed by all employees. If the security policy has not be implemented or communicated effectively across the organization and signed by all employees, it might leave the company vulnerable to laptop and data theft. A security policy is a formal document to be read by employees so that security practices can be standardized and agreed upon by them.

What is the need for a laptop security policy?

Cutthroat competition in every sector and the increasing instances of data and identity theft has brought the need for data security has come to the notice of governments across the world. With more and more organizations leveraging the fact that laptops enable them to increase their mobile workforce, specific security measures that differ from those for desktop PCs, which are always under the control of the company, need to be put in place.

Computer forensic experts have found that 70% of laptop users do not conform to any laptop security policy. With only 30% of the people following basic security measures, there has been an increase in the rate of laptop theft cases. One case that was in the news was the data theft at ChoicePoint Inc. in 2005, when more than 35,000 customers in California alone reported theft of personal information.

Understanding the reality that mobile computers are security risks, end users should be aware of the laptop security policy. Apart from that stolen data, laptops impact the financial structure by increasing expenses associated with the replacement of hardware and software. More than anything else, it is the risk to the reputation of the organization when proprietary information and intellectual property is accessed by unauthorized users and the threat of potential lawsuits that make investment in security measures crucial.

What does a laptop security policy consist of?

Although more and more organizations are choosing to issue laptops to their staff, most companies do not put in place a security policy that holds employees accountable for these machines. Laptop theft leads not only to material loss, but the loss of sensitive data stored in the laptop can expose the organization to various problems, including legal action taken by the affected parties.

Various factors need to be considered while formulating a laptop security policy:

- The agreement stating laptop security policy of an organization should comprise of security measures not only regarding hardware but software as well.

- As far as hardware security is concerned, companies can restrict the use of certain

peripherals, such as CD-drives, USB flash drives, etc.

- ☐ All employees should agree to conform to the guidelines regarding the installation and scheduled upgrade of anti-virus software and firewalls, with the purpose of protecting confidential data.
- ☐ The use of encryption software is essential to prevent unauthorized access to sensitive information.
- ☐ Recommendations regarding internet use should also be stated in the security policy.
- ☐ The security policy should allow only authorized or legitimate users to access the network and resources.
- ☐ Most important of all, the working environment of an organization has to be kept in mind while framing the laptop security policy. Depending upon the work culture, the security policy of different organizations can differ in regulations and standards.

Further, one basic point that should be stressed upon is that all the practices to be conformed to should be mentioned in a manner that is understandable to all employees of the organization. Various other legal and statutory implications have to be considered while framing the laptop security policy. Apart from these, the security policy of business partners as well as industry norms might also play an important role in the formation of laptop security policy.

All good security policies have three basic characteristics:

1. They are enforceable.
2. They provide accountability
3. Each clause is measurable/auditable to ensure that the policy is adhered to

Who Should Know About This Policy?

Just as every driver needs to be aware of the rules of road traffic, every member of an organization with access to the resources of network and database management should be aware of the laptop security policy. All the employees, including those working from home, should be made to sign the security policy of the company. Moreover, the security policy should be shared with contractors, visitors, business partners and customers who are given access to the network so that proper security can be maintained.

A lot depends on the well written and clearly communicated security policy that will enable employees to implement the security measures effectively, reducing the risk of theft. Responsibilities and obligations of employees should clearly be stated in the policy and there should not be any ambiguity that might lead to any kind of misunderstanding.

Conclusion

Since security is one of the major concerns of any organization that uses complex computer networks, centralized administration of all data stored within these networks is essential. Administrative controls can include keeping a check on all laptops issued by the company, ensuring regular updates for antivirus, firewall and encryption software, ensuring that all employees understand and adhere to the security practices outlined by the policy, etc.

The security policy also needs to be audited from time to time so that any developments in technology or changes in the nation's data security legislation can be incorporated. Organizations also need to put in place powerful mechanisms to ensure the implementation of the security policy.

There should be audit trials conducted either by the IT professionals of the organization or third parties to test the security policy. The security policy should also include a contingency plan that needs to be followed in the event of laptop or data theft.