Information security policy: development guide for large and small companies

Technology, Information Technology

Information Security Policy: Development Guide for Large and Small Companies

Information security laws and practices involve the ways of ensuring that organizations protect and manages their information, that is, in a confidential and safe manner, in order to prevent it from getting lost or being distorted for the purpose of achieving laid goals. The government, organizations and businesses should be careful in the way they disseminate or disclose information. These include practices such as preventing any unauthorized personnel from such delicate sources, use or alteration of information.

Businesses, the government and organizations should establish appropriate policies. These include a number of set procedures or rules concerning information which have to be observed by all staff in order to ensure that organizational information remain safe and always available for use . (Microsoft, 2009). This therefore limits the staff on the extent to which they can go to reach certain information in organizations. They also receive only the relevant information and by this doing, the entire organization’s information is made available, confidential and of adequate data integrity. (Danchev, 2003)

Policies are in two categories when it comes to information security in any organization. Organizational policies and government policies. The organizational policies are made to set protocol in organizations while the government policies rule those in government offices and are normally set by the state. (British Columbia, 2011). For instance, organizational policies must protect the entire staff and their information resources or tools, set the

ethical standards expected of all employees and also set due acts of punishment for all the violators of the set policies so that they can follow these policies to the latter. (Canavan and Diver, 2007).

Regulations are the second set of rules in an organization or government. Their purpose in these institutions is to prohibit allows something to take place. By this, they therefore reduce occurrences of any risks when it comes to information security as opposed to its loss or distortion. (Danchev, 2003).

Laws constitute the last category of rules. They can either be public laws or private laws. Private law works between the organization and the employee while public laws rule the entire government, its people, and all the employees in an organization. (Whitman and Mattord, 2007).

Legal environment comprise of the relevant polices; laws and regulations have been found to have a great impact in organizations. They much influence attributes such as integrity, availability of information and information systems and confidentiality in many organizations in the following ways.

Data integrity in an organization means that the information is correct and by this doing, organizations can be accurate and consistent in the way they serve their customers or clients. Secondly, minimum errors in information will be experienced if governments and organizations come up with laws that put much enforce integrity of data.

Government and other organizations must in a way design on ways of ensuring confidentiality in their information in other words preventing unnecessary disclosure of information . This mostly applies to the information and technology devices they use or by word of mouth, print and

e-mailing the information to a second party. For instance, any unauthorized access to such devices and information or data should be prohibited for maximum information security. Any information about a business' customers, the organization itself or government must never be spread out because it may in one way or another lead to bad reputation from the public and such organizations or businesses may experience massive losses in customers thus leading to low profits.

Availability of useful information in an organization or government enables due attainment of the set goals because such kept records act as sources of references and that the information can be accessible when needed. If this is enabled, then there is no doubt that these institutions can develop and become competitive with time. In enhancing availability of information, organizations are advised to use antivirus software which scans the stored data in computers. (Evans, 2006).

References

1. Canavan, C. & Diver, D. (2007). Information Security Policy – A Development Guide for Large and Small Companies. SANS Institute , SI: SANS Institute publishers

2. Columbia, C. (2011). Information Security Policy. British Columbia, BC: Capital press

3. Danchev, D. (2003). Building and Implementing a Successful Information Security Policy. Washington, DC: New media

4. Evans, E. (2006). Securing a Web Site. United States of America, U. S. A: McKay press

5. Microsoft, M. (2009). Software Use Policy. New York, NY: Microsoft

publishers

6. Whitman, W. & Mattord, M. (2007). Legal, Ethical, and Professional Issues in Information Security. Washington, DC: New media