Chapter 34

Organizational Software Use Policies

Alex Ozoemelem Obuh
Delta State University, Nigeria

ABSTRACT

This chapter discusses organizational software use policies. Specifically it gives the meaning of software use policy, software use policy components bothering on; general statement of policy, user education, budgeting and acquisition of software, registration, installation, storage and documentation of software, record keeping, software use, internet and shareware use, software audit and use survey, employee/user duty to report underlicensing, disciplinary measures on defaulters, corporate handling of employee questions regarding an organization's software, need for software use policy in an organization, organizational software use policy formulation process, qualities of a software use policy, policy education and enforcement, problems of software use policy as well as future trends in organizational software use policy.

INTRODUCTION

The Internet has made possible quick and easy access to software downloads but there are accompanying consequences to guard against, such as acquiring malware/malicious payload which can cripple an entire organization's information system, software piracy which can lead to poor quality/standard of software, etc. (Obuh, 2008). Software programs are protected through patents,

copyright, trade secrets and trademarks; violation of which can attract severe sanctions as provided by the appropriate laws. Hence it is imperative for users/organizations to provide adequate policies on software use. The purpose of this policy is to prevent copyright infringement and to ensure proper software asset management (Foltz, Cronan & Jones (2005).

According to Foltz, Cronan & Jones (2005), the following questions suggest today's organizational scenario: did you read the software license agreement the last time you installed software

on a personal computer (PC)? What about the computer usage policy for your organization: have you read it? If you answered no to these questions, you are not alone. Although many individuals in organizations have read (and often sign) software use policies explaining acceptable and unacceptable uses of organizational computer software components, the cost and frequency of information systems misuse and computer crime continue to rise. This paper intend bringing to the fore, understanding of computer software usage policies of corporate organizations.

BACKGROUND

At this point it is pertinent to define the following the terms 'policy', 'software' and 'software policy'. A *policy* is a deliberate plan of action to guide decisions and achieve rational outcome(s) (Adomi, 2008). Policy helps to define what is considered valuable, and specifies what steps should be taken to safeguard those assets (Gafinkel & Spafford 1996). Policy is defined as the set of laws, rules, practices, norms, and fashions that regulate how an organization manages, protects, and distributes sensitive information, and that regulates how an organization protects system services. (Longley & Shain, 1990; DoDCSEC 1985). The term policy may apply to individuals, government, private sector organizations and groups. Presidential executive orders, corporate privacy policies, and parliamentary rules of order are all examples of policy. Policy differs from rules or law. While law can compel or prohibit behaviors (e.g. a law requiring the payment of taxes on income) policy merely guides actions toward those that are most likely to achieve a desired outcome Longley & Shain, 1990; DoDCSEC 1985; Dijker, 1996).

Policy may also refer to the process of making important organizational decisions, including the identification of different alternatives such as programs or spending priorities, and choosing among them on the basis of the impact they will have.

Policies can be understood as political, management, financial, and administrative mechanisms arranged to reach explicit goals (Gafinkel & Spafford 1996). Access to a system may be granted only if the appropriate clearances are presented. Policy defines the clearance levels that are needed by system subjects to access objects (DoDISPR, 1982). In an access control model, policy specifies the access rules for an access control framework (Kao & Chow, 1995).

Software is a set of instructions that cause a computer to perform one or more tasks. The set of instructions is often called a program. Computers cannot do any useful work without instructions from software; thus a combination of software and hardware (the computer) is necessary to do any computerized work. The term *software* applies to application programs, specialized system programs, or operating system utilities (which relates to operating the computer system). Software packages are available for many accounting-related applications, including bookkeeping, tax preparation and planning, management advisory services, audit, spreadsheets, data base management, preparing formal reports and documents, and practice administration (i.e., time and billing) (Obuh, 2008).

Software policy will make it clear to employees what types of software (if any) they are allowed to download and install for use on their company PC or mobile device, and whether or not such downloads need to be cleared by the IT department. According to Krsul (1998), such a policy is the set of rules that define the acceptable value of a system as its state changes through time. In operating systems such as Unix and Windows NT, the security policies that can be enforced by the operating system are a subset of the policies that users and administrators expect applications and the system to enforce.

Protecting against malware should be one concern. Freeware and shareware applications can deliver malicious payloads to corporate PCs and networks. Software piracy should be another

Related Content

Regulation of Cybercafés in Nigeria

Mercy Eyitemi (2011). *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements (pp. 590-598).*

www.irma-international.org/chapter/regulation-cybercafés-nigeria/45411

Market Response to ISO 9000 Certification of Software Engineering Processes

G. Keith Fullerand Ilan Vertinsky (2006). *International Journal of IT Standards and Standardization Research (pp. 43-54).*

www.irma-international.org/article/market-response-iso-9000-certification/2577

Profiles and Motivations of Standardization Players

Cesare A. F. Riillo (2013). *International Journal of IT Standards and Standardization Research (pp. 17-33).*

www.irma-international.org/article/profiles-and-motivations-of-standardization-players/83545

An Access Control Model for Dynamic VR Applications

Adam Wójtowiczand Wojciech Cellary (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 857-878).*

www.irma-international.org/chapter/access-control-model-dynamic-applications/75060

What, Me, Worry? The Empowerment of Employees

Marsha Cook Woodbury (2004). *Social, Ethical and Policy Implications of Information Technology (pp. 59-73).*

www.irma-international.org/chapter/worry-empowerment-employees/29306