



Computer Systems Policy Excerpt

The following is an extract from the ICT Policy constructed by I.T. Aid.
(Full document available on request.)

Computer Systems Policy and User Guide

This document establishes computer usage guidelines for (COMPANY NAME) staff in the course of their job duties on (COMPANY NAME) computer systems. These guidelines are intended to protect the rights and privacy of (COMPANY NAME) clients as well as those of (COMPANY NAME) staff. Members of staff are required to abide by all the items outlined in this document. Certain members of the (COMPANY NAME) staff have some level of special access. Special access is defined as having the password to access specific data (eg. accounts or sales data) on a (COMPANY NAME) computer. The document also specifies behaviours and practices that are prohibited. All members of staff should reference this document whenever they have a question regarding proper use of the company's computer systems. Data Protection

The Data Protection Act 1998 is concerned with the processing of computerized and manual information about living individuals (personal data) and gives rights of access to the individuals who are the subject of that information. Further, the Act places certain obligations on (COMPANY NAME)'s data user, in respect of the personal information it processes or causes to be processed on its behalf by third parties. Acceptable Use Statement

The following document outlines guidelines for use of the computing systems located at or operated by (COMPANY NAME). Computing systems will include any computer, server or network provided or supported by (COMPANY NAME). Use of the computer systems includes the use of data/programs stored on company computer systems, data/programs stored on magnetic tape, floppy disk, CD ROM or other storage media that is owned and maintained by the (COMPANY NAME). All data/programs on company computer systems are the property of (COMPANY NAME) and as such must remain on (COMPANY NAME) computer systems in the event of, for whatever reason, the termination of employment of a member of staff.

The 'user' of the system is the person requesting an account (or accounts) in order to perform work in support of (COMPANY NAME). The purpose of these guidelines is to ensure that all (COMPANY NAME) users use the computing systems in an effective, efficient, ethical and lawful manner.

(COMPANY NAME) accounts are to be used only for the purpose for which they are authorised and are not to be used for non (COMPANY NAME) related activities. Users are responsible for protecting any information used and/or stored on their (COMPANY NAME) computers.

Users are requested to report any weaknesses in (COMPANY NAME) computer security, any incidents of possible misuse or violation of this policy to the system administrator in person or by sending electronic mail to support@itaideurope.com

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized (COMPANY NAME) user access to a (COMPANY NAME) resource; obtain extra resources, beyond those allocated; circumvent (COMPANY NAME) computer security measures or gain access to a (COMPANY NAME) system for which proper authorisation has not been given.

Users shall not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, (COMPANY NAME) users shall not run password-cracking programs on (COMPANY NAME) computer systems.

Any non compliance with these requirements will constitute a security violation and will be reported to the management of (COMPANY NAME).