

Example (Generic) Unauthorised Software Policy



Introduction

The company relies heavily on telecommunications and computers, so it is vital that it is protected against the threats posed by computer virus attacks and the infringement of intellectual property rights. The following gives some guidance on the interpretation of the policy and procedure.

Procedure

1. The IT manager should ensure that she/he institutes controls to prevent any software being used on company computers without her/his authority. In the context of this procedure, software is used if it is loaded, executed or copied from or with the said company computer.
2. In instituting controls the IT manager should consider the costs and benefits involved. For computers running business critical applications, sophisticated access control techniques will be appropriate. For normal PCs physical security precautions supported by reasonable observation and periodic review of hard disks for unauthorised software, should be sufficient.

Guidance for the IT Manager

1. In the case of mainframe or mid-range computers which run several applications, there may be several staff each looking after one or more application. There should, however, be one member of staff with overall responsibility for the mainframe or group of related computers. She/he may delegate some of her/his tasks to others but should retain accountability.
2. In the case of personal computers (PCs), the IT manager will usually divide the responsibilities between a departmental administrative/control function and the prime user of each PC. Such arrangements are entirely at the discretion of the IT manager so long as all staff concerned know their responsibilities and between them ensure that the policy is adhered to.
3. Where a PC is shared between several users, no one of which is obviously the prime user, the IT manager should nominate a user or another member of staff to fulfil the prime user's role.
4. The IT manager should arrange for a periodic review of all computers. This should include company computers held off-site by members of staff.
5. The IT manager may consider software to be properly licensed if she/he has in her/his possession a valid licence for the software to be used on the company computer. This includes evaluation copies, which may have a limited-use licence. If there is a limit on the number of copies that may be used, it is the responsibility of the holder of the multi-user licence to ensure that this number is not exceeded.

Example (Generic) Unauthorised Software Policy



6. Where a PC is attached to a network, it is the responsibility of the administrator of the network server to ensure that software on the server is properly obtained, licensed and tested.
7. Some games software can be used for a valid company business purpose, such as teaching keyboard skills. Use of such software may be authorised if it meets the other criteria set out in the policy and the purpose has been approved by the IT manager. Otherwise, games and applications which relate to non-company activities should not be authorised.
8. Some software packages which are used for valid company business purposes contain games (e.g. Microsoft Windows contains Solitaire). Use of these facilities during working hours should be discouraged.
9. Software may be considered to have been properly acquired if this has been developed by company or purchased by company through the approved purchase process. Software available free or cheaply from the Internet, through bulletin boards or computer clubs should not be used unless a good business case can be made and approval is obtained from the IT manager.
10. It is advisable to examine carefully all purchased software on an isolated computer which contains no critical or sensitive files before use. Where no such computer is available in one department, the facilities of another department should be used where practical. As with all testing, the degree of care taken should be risk based.
11. Normal acceptance testing should be sufficient to detect viruses in bespoke or customised software. PC software obtained “shrink wrapped” from a reputable supplier may be considered to be low risk. PC software obtained on courses or at exhibitions (e.g. demo disks) should be considered to be of higher risk and software received unsolicited, through the post or with a magazine, even higher risk. Higher risk software must be examined and passed by appropriately qualified staff on an isolated machine before use on any other company computer.
12. In general, staff and contractors are not permitted to run their own software on a company computer. If there is a valid business purpose which can best be satisfied by using software for which company does not hold a licence, then a business case should be made and the software acquired through an approved company purchase process. If the IT manager believes that there is a valid business case for a member of staff or a contractor to use his own software on a company computer, the manager must:
 - obtain evidence that the user has a valid licence to use the software for the intended purpose on company equipment;
 - ensure that the software is appropriately tested before it is loaded onto company equipment;
 - periodically check that the user continues to hold a valid licence; and
 - ensure that the software is deleted as soon as the user leaves company or ceases to hold a valid licence for the software.