Dorset County Council

IT Security Policy and Standards

Version no: 1.0

1 December 2005

Document revision history:

Date	Version	Description
1 December 2005	1.0	Replaces IT Security Standards (October 2002 version)

IT Security Policy and Standards

1. Policy Statement

The work of the County Council is increasingly reliant upon Information Technology (IT) and the data held on computer systems, be they Corporate or locally based. It is crucial that such data is accurate, secure and confidential. The computer equipment required to process that data must always be available for use and, as far as possible, always be in a properly functional state. If either premise is untrue, then inconvenience will and financial loss may occur.

All IT systems, and the Electronic Document and Records Management (EDRM) system in particular as a corporate repository for the Council's electronic records, will be configured, as far as is possible, and administered with due care, to protect the integrity, authenticity and appropriate levels of confidentiality of records.

Although IT Services will always endeavour to take measures to satisfy these aims, they cannot be achieved without the active support of the User. In order that data, equipment and systems may be maintained in a sensibly controlled environment there are a number of steps that must be taken. These are set out below.

2. Scope

This document replaces the IT Security Standards (October 2002 Version). It relates to the use of any IT services irrespective of the equipment or facility in use. It applies throughout the County Council and to all who use the facilities.

The 'Peoples Network', which is available to members of the public in libraries, is covered by an 'Acceptable Use Policy' and not by this policy.

3. General

1. IT security is the responsibility of the County Council as a corporate entity and all members of staff who use computer equipment and systems.
2. The County Council has to abide with all UK legislation affecting IT. All staff must comply with the following Acts and may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted:
    - Data Protection Act 1998
    - Freedom of Information Act 2000
    - Copyright and Related Rights Regulations 2003
    - Computer Misuse Act, 1990
3. The County Council aims to comply with ISO 17799, the international standard for information security management. This is particularly relevant as far as EDRM is concerned.
4. Directors must ensure that every member of staff using computer equipment or systems is given a copy of these Standards and retain signed acknowledgements from staff to this effect.
5. Any violation of these Standards or any suspicion that unauthorised access has occurred or equipment has been tampered with must be reported to the Director or his designated officer, who should report it to the Head of ICT Strategy and Systems immediately. **Non compliance with these Standards may be considered as misconduct (either ordinary or gross) and will be dealt with under the Disciplinary Procedure.**
6. These Standards may be modified from time to time, in response to changing circumstances, of an operational, legislative or technological nature.

7. Periodic checks will be made by Directors, their designated officers, the Head of ICT Strategy and Systems, his representative or the Director of Resources Computer Audit staff to ensure compliance with these Standards. Where required to do so staff must disclose passwords for this purpose.

8. Any person requiring clarification or further advice should, in the first instance, contact the Director or his designated officer who may consult IT Services if necessary.

4. Computer Equipment

1. Directors are responsible for the security and proper use of computer equipment within their directorates, including establishments. Where they designate specific officers responsible for specific equipment and systems, then such delegations must be recorded and that record must be kept up to date.

2. No computer equipment is to be set up for connection to the network or for attaching to any equipment connected to the network, without the authorisation of the Head of ICT Strategy and Systems or an officer designated by him. Networked computer equipment must only be moved by IT Services staff, IT Liaison Officers or other authorised staff.

3. All new network connections to County Hall from external DCC sites or external agencies must be routed through the corporate firewall system to ensure the integrity of the core network and systems.

4. In accordance with Financial Regulations, all moveable equipment shall, as far as is practical, be marked as County Council property and shall be recorded in the appropriate directorate or establishment inventory and in the County Council's corporate database of IT equipment and software maintained by IT Services.

5. Official County Council equipment, including portable and laptop computers, shall be used for official purposes only, except where specifically permitted. No private work may be carried-out or private material stored on it. (See also paragraphs 7.3 and 7.4 below.)

6. Only persons authorised by a properly designated officer may use computer equipment.

7. All computer equipment must be secured from theft or unauthorised use as far as is practical.

8. Where stolen equipment and/or software are recovered; or where it is suspected that equipment or software has been tampered with, then they must be tested by IT Services prior to re-use.

9. Suitable fire extinguishers must be provided close to all computer equipment.

10. Computing equipment is extremely sensitive and great care must be taken to avoid accidental damage, especially when eating or drinking close to such equipment.

11. Computer stationery of a sensitive nature (e.g. blank pre-printed cheques or blank stationery for computer-produced orders or receipts) must be securely kept. Issues must be controlled and recorded and regular physical stock checks must be independently undertaken. Advice can be obtained from Internal Audit if required.

12. Disposal of surplus equipment must be undertaken in accordance with Financial Regulations. The advice of IT Services should be sought prior to any disposal especially if sensitive data is stored on the equipment as simply deleting files does not permanently remove them. All software and data must be removed from IT equipment before disposal.

5. Software and Data

1. Only officially approved software may be run and if the application uses the network, the Head of ICT Strategy and Systems must be informed. In this context, “officially approved” refers to software applications that are supported or approved by IT Services or by a Directorate’s own IT Liaison staff. If software has not been approved by IT Services, Directorate IT Liaison staff must ensure that the application is designed for the computer’s operating system and network and will not impact upon the

reliability or security of the computer or network. Advice should be sought from IT Services if in doubt.

2. Installation of software (including screensavers) from any source must only be carried out with prior authorisation from IT Services or directorate IT liaison staff.
3. Only screensavers supplied with a workstation's supported operating system (e.g. Windows NT) may be used except where alternatives have been specifically ratified. Directorate IT Liaison staff may request that IT Services ratifies a very limited number of screensavers for use.
4. The use, or possession, of unlicensed copies or “pirated" versions of software is illegal and, therefore, expressly prohibited.
5. Computer games are only permitted for demonstration purposes and with permission of designated officers.
6. All demonstration, purchased or non-purchased software, software produced for the County Council and data produced for the County Council must be virus checked using County Council approved virus checking facilities before use on official County Council equipment. The use of untested software is expressly forbidden. All hardware and media acquired should be similarly checked before use.
7. All media (e.g. floppy disks, CDs) of uncertain or unreliable origin must be checked for viruses before use.
8. Where a virus is detected, the matter must be reported to IT Services immediately. Virus repair must be undertaken only by authorised and trained staff and only where the characteristics of that particular virus are known and where adequate repair is assured.
9. All facilities attached to the network are covered by the corporate virus detection and removal system. All such facilities are continuously monitored and all viruses detected are logged. The incidence of logged viruses will be monitored by Internal Audit.
10. Under no circumstances may software from bulletin boards, the Internet or other external electronic mail sources be downloaded without prior authorisation from the director or designated officer.
11. The downloading, copying, saving or transmission via email of movie clips, video clips, sound files or any similar files is not permitted unless work related. The transmission of such material internally and externally via email is not permitted.
12. All computer software developed for and data held on behalf of the County Council are for the sole use of the Council.
13. Where such software is to be written by third parties, then staff involved in negotiations must ensure that copyright is vested in the Council unless specifically authorised otherwise by the Head of IS/IT or his representative.
14. No unauthorised copying, alteration or interference with programs or data is permitted.
15. No unauthorised disclosure of computer-held information is permitted.
16. All computer data relating to living individuals is covered by Data Protection legislation. Where such data is held, then the provisions of that legislation must be followed. It is the responsibility of each Director to ensure that this is the case. Advice on compliance with Data Protection legislation is available from the Records Manager.
17. The permission of each individual must be obtained before any information about them is made available on the Intranet or to the public via the Internet. This includes photographs and personal (i.e. non-work related) details.

18. It is the responsibility of all users to ensure that any personal data to be sent complies with the provisions of the Data Protection legislation including any personal data contained in email or in an attachment to email.
19. Only with the prior approval of the Director or a designated officer may personal data be downloaded from central computing resources without written authority and only then in full compliance with any Data Protection notification, in the name of the Authority, in force at the time.
20. Appropriate security measures are to be taken for Data Protection Act sensitive information, such as access controls on internal systems and encryption for external email transmission.
21. Where data or systems are kept on portable media, such as floppy disks, then such media should be kept securely when not in use.
22. The Storage Area Network (SAN) and network servers are the only permitted storage media for EDRM.
23. Back-up copies of all data and software held on PCs and servers should be taken on a regular basis, so that all systems are recoverable in the event of damage or theft. Back-up media should be kept locked away and separate from the location of the originals. Data and software held centrally by IT Services will be secured by them.
24. Waste media (e.g. output reports, floppy disks) must be disposed of with regard to the sensitivity of the data concerned (simply deleting files does not permanently remove them) and the officially provided means of disposal should be used wherever possible.

6. Access Security

1. Users of computers attached to the network must log-out from the network at the end of each session.
2. Where such facilities are provided, terminals should be "locked" (i.e. by pressing Ctrl+Alt+Delete and Return) and in any case should never be left logged-in to a system, when left unattended. If personal computers are equipped with keyed disk locks, these must be applied when the system is unattended.
3. Passwords must never be disclosed to unauthorised persons, nor may they be displayed openly or written down in such a way as to be identifiable. If it is necessary to disclose a password to IT Staff or Directorate IT Liaison Staff to enable system maintenance or software installation etc. then that password should be changed as soon as possible thereafter.
4. Passwords or logging-on statements must never be held on function keys; nor may they be held as scripts or macros.
5. The unauthorised use of another person's password is not permitted.
6. Wherever practical, passwords should be a minimum of 6 characters in length and be changed frequently (preferably at least every 90 days) to a previously unused password. The use of "obvious" values such as people's names is discouraged.
7. Wherever practical, computer screens, unless designed for public access, should be positioned so that they cannot be overlooked by visitors or unauthorised personnel. Authorised screen savers should also be used.
8. Information concerning computer security and access methodologies must not be divulged to unauthorised persons.
9. Officers using computing equipment away from the workplace are responsible for the security of that equipment and for the data held on it. They must ensure compliance with these Standards.

10. Only persons authorised by the designated officer or officers nominated by him may gain access to secure areas.
11. The transfer of "means of access" (e.g. keys, cards, electronic fobs) or disclosure of access codes to unauthorised personnel is strictly forbidden.
12. The loss of "means of access" (e.g. keys, cards, electronic fobs) must be reported to the designated officer immediately who shall at once arrange for them to be cancelled / disabled.
13. Persons leaving the employment of the Authority must return all "means of access" (e.g. keys, cards, electronic fobs), identity cards, manuals and any other property of the Council to their line manager by their last working day. All user access permissions must be de-activated or cancelled at the same time.
14. All visits to secure areas must be appropriately recorded and authorised.
15. Staff using personal computer facilities for official work should only do so in accordance with arrangements approved by the appropriate Director who must ensure that these Security Standards are complied with particularly in relation to Data Protection.
16. Any known or suspected IT security breach or threat must be reported to IT Services at the earliest opportunity. The procedures covering this are given on the IT Security Incidents page on the Intranet.

7. Internet Access / Electronic Mail

1. Staff must use the Corporate Internet connection, *not individual dial-up connections*, to access the Internet.
2. In exceptional circumstances, requests for individual dial-up connections should be forwarded to the appropriate Director and Head of ICT Strategy and Systems. All machines used to download data or files from the Internet via dial-up connections must have up to date virus checking software installed. Any files so downloaded must be checked for viruses before they are used or passed on elsewhere.
3. Internet access is provided for official business. Personal use of individual dial up connections is not permitted. Personal use of the Corporate Internet connection by staff is permitted but this must be in their own private time and at no extra cost to the Authority. Except in trivial cases the use of disk storage (either locally or on a server) and printing facilities etc is for official purposes only. All traffic via the Corporate Internet connection is logged and will be subject to monitoring without prior notice. Staff are reminded of the facilities available within public libraries which are not subject to monitoring at individual user level.
4. The Corporate email system is provided for official business. Personal use is permitted provided it does not violate these Standards and does not hamper or conflict with official business. The County Council retains the right to view and monitor all email created, sent, forwarded, received or saved on the corporate email system without prior notice. Staff are therefore advised to think carefully before using it to communicate personally sensitive information.
5. The County Council accepts no liability for any consequences (including financial or other loss) which may arise through private use of the corporate Internet or email facilities.
6. The Internet connection has a finite capacity and users of the service must be sympathetic to this and not degrade performance by browsing or downloading unnecessarily large amounts of information. To this end, the facility to download files or video will not be generally available. These facilities can be made available by IT Services on request through your Directorate Web Manager.
7. County facilities may only be used for lawful purposes. Viewing or transmission of any material which may be regarded as offensive or in violation of any UK law or regulation is not permitted. Such material may include copyright material, material judged to be threatening, sexually explicit or obscene and material protected by trade secret.

8. Sending an email, or attaching a file to an email, constitutes processing of personal data if there is any personal data on a living individual within the email or the attachment. Such processing can only be undertaken if it is permitted under the Authority's data protection notification.

9. Nothing must be published that might bring discredit or harm to the Authority, its officers or members or might bring the Authority into disrepute.

10. All incoming information must be continually monitored for viruses. Where an incoming virus is detected, or some other problem appears to have been caused as a result of email received, the matter must be reported to IT Services immediately. Virus repair must be undertaken only by authorised and trained staff and only where the characteristics of that particular virus are known and where adequate repair is assured. Facilities attached to the network are automatically monitored for viruses.

11. All messages transmitted to the Internet from the Corporate email system shall have the following automatically appended:-

    "Please note that the content of this message is confidential between the original sender and the intended recipient(s) of the message. If you are not an intended recipient and/or have received this message in error, kindly disregard the content of the message and return it to the original sender."

12. Care must be exercised when sending emails with large file attachments as they consume large amounts of network capacity and impact on the overall network and email system performance. This is particularly the case when sending to the Internet or to other DCC offices outside of the sender's location.

13. Junk email (such as that containing, or having an attachment containing, jokes) from both internal and external sources should be deleted and only forwarded to another person if they have a genuine use for it.

14. Recipients of "chain email" should delete any such messages and attachments received and should not participate in the onward transmission of such material.

15. The downloading, copying, or transmission via email of executable files (e.g. Those with a ".exe" file extension) is not permitted without the authorisation of IT Services or Directorate IT Liaison staff. File attachments from suspicious or unknown sources should not be opened.

16. Email should not be used for the transmission of sensitive and confidential information unless confidentiality and integrity during transmission can be guaranteed and the recipient is capable of authenticating the source.

17. Internet or email facilities should not be used to order official goods and services except in circumstances approved by the Director of Resources.

18. Guidance on the use of email within Dorset County Council is contained in the Communications Unit Guide to Using Email.

8. IT Security Framework

1. IT security is the responsibility of the County Council as a corporate entity as well as all those who make use of its computer equipment and systems.

2. Designated support personnel within IT Services are responsible for the monitoring of IT security threats as well as the monitoring of IT security breaches.

3. The IT Services Operational Management Team reviews any significant operational issues, including those relating to IT security.

4. The IT Services Security Group, which includes representation from both the IT areas referred to earlier in this section, meet on a regular basis to discuss any IT security issues of concern, make

recommendations to IT management, review technology related audit recommendations and deal with issues referred from the corporate ICT Security Group.

5. The corporate ICT Security Group consists of representation from IT Services, as well as from each Directorate. The responsibilities of this group include reviewing the 'IT Security Policy and Standards', making recommendations in relation to this policy and other IT security issues, reviewing IT security audit recommendations and ensuring, as far as they are able, that their Directorate are aware of, and comply with, all relevant IT security policies and procedures.

6. The Information Systems Strategy Group (ISSG), with appropriate advice from Internal Audit, is responsible for recommending to County Management Team any changes to the 'IT Security Policy and Standards'. This group also has responsibility for endorsing any initiatives to improve IT security that have been recommended by the ICT Security Group.