



TENDRING DISTRICT COUNCIL

INFORMATION TECHNOLOGY SECURITY POLICY

Prepared By: ICT Services

INFORMATION TECHNOLOGY SECURITY POLICY

Main Objective

In order to minimise any adverse risk to the Authority, the Council will establish and operate the effective controls and procedures, detailed in this document, to protect the authority's IT systems infrastructure, hardware, software and information, to ensure that they are kept secure and only available for proper and authorised utilisation.

Scope of The Policy

The IT Security Policy will encompass the following :-

1. Security Policy Authority
2. Definition of responsibilities for all aspects of this security policy
3. Asset control
4. Personnel security issues
5. Monitoring and Management controls
6. Physical and Environmental security
7. Hardware and Network management
8. Anti-virus controls
9. Central IT Help Desk Facility
10. System and Access controls
11. System development and maintenance standards
12. Disaster recovery
13. Compliance with legislation
14. Data utilisation control and media handling
15. Project implementation and review

1. Security Policy Authority

The Security Policy will be developed and approved in conjunction with the IT Sub-Committee and fully endorsed and supported by the Council's Management Board and Heads of Service.

2. Definition of responsibilities for all aspects of this security policy

2.1 The Council

The Council (Members, Management Board, Heads of Service and all personnel), all Third Party Contractors (ie. IT FM Supplier) and Sub Contractors shall be bound to ensure compliance with all aspects of this security policy by the implementation of effective compliant procedures and measures within their own areas of responsibility.

2.2 IT Services

IT Services (Technical and Procurement Unit) shall be responsible for the:

- definition and development of the Security Policy and the regular review of its effectiveness;
- definition of the procedures and technical standards relating to those IT services supplied by Third Party Contractors;
- specification, or assistance with, Tender documentation for IT or IT related services;
- corporate IT procurement;
- definition of operational guidelines for authorised Council users of Authorities hardware and software systems;
- implementation of procedures to enable compliance with Data Protection Act and associated legislation;
- implementation of system/application access guidelines to prevent unauthorised access and monitoring of usage;
- provision of effective corporate anti-virus utility software;
- provision of "Fire Wall" network security;
- provision of an effective Backup and Disaster Recovery operation.

2.3 IT FM Supplier and Other Third Party Contractors

The Council's IT FM Supplier (The Supplier) is responsible for implementing adequate security measures to prevent unauthorised access to systems and applications and also to detect security breaches or attempted security breaches where they have occurred. All development User passwords will be secured and maintained by The Supplier, to a standard agreed by The Council.

The Supplier shall maintain physical security of all areas used by him in the provision of the Services and implement appropriate security safeguards (both physical and software) against destruction or loss, unauthorised use, access or alteration of Data and Software.

The Supplier shall monitor all system access, security/protective measures on a day to day basis, reporting any incidents to The Council immediately they occur.

The Council's IT FM Supplier and other Third Party Suppliers are responsible for supplying all contracted IT services in accordance with the appropriate IT Services Agreements and in full compliance with this Security Policy.

All Third Party IT Service suppliers have full responsibility for ensuring that any sub-contractor or other Third Party supplier invited onto Council premises, understands and fully complies with all safety, security and working procedures.

The IT FM Supplier is responsible for all the day-to-day operations as defined within the IT Services Agreement (ITSA).

The IT FM Supplier shall provide access to their Data Centres for the Council's IT Services Team and the Council's Internal Audit staff to allow periodic review of the security and procedures in operation by The Suppliers' personnel who are engaged in working on the Council's systems.

The Supplier will positively assist the Council to comply with it's policies relating to Information Technology as set out below. The Supplier will not undertake any actions, unless authorised to do so by the The Council's IT Services Team, that will result in the failure to comply with any security requirement in respect of any related matters detailed below.

- Access to systems
- Back up of data and systems to tape.
- Virus protection.
- Database integrity of Mainframe systems
- Access to Mainframe system user and switch user facilities
- Disaster Recovery and contingency planning
- Hardware inventory maintenance, Electrical Testing and Health and Safety procedures.

The employees or subcontractors of any Supplier will be expected to comply with all instructions from the Councils Safety Officer or his representatives.

2.4 System Sponsors

Individual system sponsors are responsible for managing the day to day secure authorised use of their specific IT system as authorised by the Council and to initiate management processes to ensure that all staff under their management fully comply with this policy.

2.5 Authorised Users

Each and every authorised user of any system has an individual responsibility to ensure that their own use of the Council's hardware, software, applications and information is for proper, authorised purposes only. Each person has a responsibility for compliance with the Data Protection Act and to protect the information, facilities and privileges afforded to them.

Equipment is only to be used for purposes directly concerned with the Council.

Council staff must only carry out operations to, and functions of, the computer equipment for which they are authorised.

Council staff must not disclose or make use of information not available generally to the public, which they may acquire in the course of their duties.

3. Asset Control

In order to maintain effective protection and control of physical I.T. assets an inventory of all I.T. equipment owned or operated by the Council shall be maintained by The Supplier on behalf of the council and made accessible at all times. The inventory shall include the following minimum detail :-

- inventory number and serial number
- manufacturer and/or supplier
- warranty/maintenance details
- supply date
- network details
- user and location details
- configuration details
- modem installations (where applicable)

All installations, relocations or re-installations of hardware or software shall be subject to authorisation by the IS/IT Manager, his deputy or a nominated representative.

All IT acquisitions, purchases and/or developments shall be requested by the individual Head of Service concerned and shall :

- submit a supporting business case for consideration and proper approval by the appropriate authority :
 - Head of Technical and Procurement
 - Management Board
 - IT Sub-Committee
- be the subject of immediate notification to the Insurance Officer once purchased.
- labelled and marked for security purposes and ease of identification where appropriate.

4. Personnel Security Issues

All issues relating to the use of IT by the Council's authorised personnel :

- will be addressed at recruitment stage by the appropriate reference and qualification verification.
- User training - all Staff Induction Courses include Data Protection Act awareness.
- Ongoing IT skill training programmes are provided along with guidance on the correct use of IT facilities, supported by Personnel and Management Services Computer Use Policy and Application Help Guides/Guidance Notes.

5. Monitoring and Management Controls

This is the process of controlling the release and change of the constituent items of the Hardware, Software and Network, and any associated documentation. Its purpose is to ensure that, despite the implementation of changes, systems are available to the Council's users. The following principles will be applied :-

- Change control procedures shall be operated in respect of initiation of, implementation of, amendments to and development of IT hardware and/or software to ensure all such actions are subject to the appropriate authorisation and documentation.
- Test environments will be developed and operated, where appropriate, and be utilised for testing and validation of new and/or upgraded software material.
- The change must be implemented in a manner that minimises disruption to Services.
- The means shall be made available to revert to known working systems in the event of any change or amendment causing a loss of, or degradation to, services.
- No change and/or amendment to any system will be allowed to jeopardise the full operational success of any other related systems or services.
- Any change will be fully documented and, where applicable, will be incorporated into the Council's IT FM Agreement in accordance with Schedule 4 of the ITSA.

6. Physical and Environmental Security

6.1 Physically secure areas

All Council personnel and Third Party Contractors (ie. FM Supplier) shall maintain physical security of all areas used by them in the provision and use of Services and implement appropriate security safeguards against destruction or loss, unauthorised use, access to or alteration of Hardware, Software, Data and Hard copy (printed) information.

6.2 Equipment security standards

- All IT Equipment will, wherever possible, be located within Staff Only areas which are protected by door entry systems.
- Any item of IT Equipment located within an area open to the public will be physically secured to either the fabric of the building or to a substantial piece of furniture.
- Entry controls will be sited on all areas where high value equipment and/or sensitive data is stored (ie. Main computer Room, Server Room).
- Air conditioning, Uninterrupted Power Supply (UPS), clean power supply, intruder alarm and fire alarm will be located on the main computer room.
- IT Equipment must not be removed from Council premises without the permission of the IS/IT Manager and the staff member's Head of Service who must maintain a log of who has what at any time. In addition, any IT equipment removed from Council premises must first obtain approval from the Council's Insurance Officer.
- The IT FM Supplier must be informed of all laptops and other portable equipment, along with the name of the regular user, for entry onto the Council's hardware inventory. Notification must also be provided to the Council's insurance officer with details of replacement value.
- To minimise the risk of theft and damage, any item of equipment removed from council premises (portable or otherwise) :
 - must not be left on display in motor vehicles
 - must not be left unattended in insecure areas
 - must not be loaned or otherwise to anyone else
 - must not be used by any unauthorised persons
 - must not have sensitive data resident on its hard disk
 - any removal of sensitive data from Council premises must be either electronically protected by password or transported in a secure container
 - care must be taken to virus check all disks and files prior to use

6.3 Cabling security

- All network cabling must be securely contained and not share trunking with any power supplies unless specifically designed to do so.
- A network map (schematic) will be maintained of all cable runs and network equipment
- A patching schedule will be maintained for each Wiring Cabinet
- All wiring cabinets will be locked to prevent unauthorised access

6.4 Computer room

The Council's computer room will be a secure and controlled environment. This environment is to be achieved by the provision of the following facilities :

- Air Conditioning suitable for the amount of equipment located in the computer room

- Fire detection and alarm system with automatic shut down and extinguishing facilities
- Intruder Alarm
- Controlled access via numeric key pads
- Water detection system
- Uninterruptable Power supply (UPS) with battery backup
- Fire alarm system in areas immediately adjacent to the computer room
- Continuous monitoring from a remote monitoring station for fire, water and intruder alarms.

The following maintenance and support contracts will be operated :

- Air Conditioning - Eaton Williams Ltd
- Fire alarms both within Computer room and for adjacent areas - GCS Alarms Ltd
- Intruder and water detection alarms - GCS Alarms Ltd
- UPS and battery back up - Leibert Ltd
- Telephone link to monitoring station - British Telecom
- Provision of a monitoring station - GCS Alarms Ltd

In addition to the above, the following will apply :

- After office hours when the computer room is unoccupied the intruder alarm will be activated.
- Only authorised personnel will be given unattended access to the computer room. All other personnel must be accompanied at all times by an authorised person.
- The Council will be responsible for determining who is authorised to have access to the computer room.
- All equipment located within the computer room will be connected to the electricity supply via the clean supply which has UPS and battery backup.

7. Hardware and Network Management

Operational procedures and responsibilities :

- Documented operating procedures for the operation of all computer systems will be maintained.
- Segregation/diversification of duties will be operated, where appropriate, by all System Sponsors to minimise any risk of negligent or deliberate system misuse.
- Separation of development and operational facilities to provide a non-live environment for any development or testing without risk to the live system and service delivery.

8. Anti-virus Controls

Protection from malicious software.

8.1 Virus controls

- IT Services will provide anti-virus software on all corporate servers and all client PCs (both networked and free standing).
- All disks received from other users, sections and/or external sources must be scanned for viruses using suitable virus protect software.

8.2 Virus procedures

The IT FM Supplier will be responsible for the regular updating and proliferation of latest virus signatures.

8.3 Virus repair software

The IT FM Supplier will be responsible for the affecting repair and recovery in the event of virus detection.

8.4 Management procedures

All suspicions of virus infection shall be immediately reported to the IT FM Supplier's Help Desk on #6599 giving all information available (ie. suspected source, type, risk, etc). The FM Supplier will inform the The Council's IT Services Team of each occurrence with full details. All information regarding virus type, source, location and remedial action taken will be recorded on the Help Desk records.

All users of the Council's IT resources shall always treat E-Mail, other data received electronically or media received via postal resources as a potential source of virus contamination; especially if the source is unknown or unexpected.

9. Central IT Help Desk Facility

- The IT FM Supplier shall operate a central Help Desk facility using The Council's software and a single telephone number (this will either be an internal Customer extension or an external number where all call costs will be the responsibility of The FM Supplier). This will be the contact / liaison point for The Council's Users even where the call/enquiry has to be referred to a third party or to the TDC IT Services team for resolution.
- All calls to the Help Desk will be logged on to The Council's computerised system by The FM Supplier. Each call will be allocated a unique reference number and all details of the call will be recorded. The exact level of detail to be recorded will be specified by the The Council's IT Services Team. The The Council's IT Services Team act

as System Sponsor for the Help Desk system and as such control the access to the system.

- The Help Desk facility shall operate and shall be manned continuously during Office Hours.
- The Council's IT Services Team will be informed immediately upon receipt of a priority 1 call and updated when such critical problems are not resolved within the target resolution times. All unresolved calls will be reviewed by The FM Suppliers Site Manager on a daily basis. The priority of the call may, at any time, be subject to reassessment by IT Services.
- Calls will be analysed by The FM Supplier to identify trends using appropriate third party software made available by IT Services. The FM Supplier will monitor faults and recommend remedial actions to IT Services with a view to improving the IT Services.
- The FM Supplier shall use the most appropriate means to broadcast information to Users relating to faults/changes, ensuring that the users are kept informed of any impact on their use of the Systems. The FM Supplier shall utilise The Council's Electronic Mail system wherever possible.
- IT Services will advise The FM Supplier of the operationally critical systems or facilities.
- All calls shall be responded to according to the specified schedule. Outstanding calls to be reviewed daily and be subject to an escalation procedure and re-classified depending on the determined impact on the user by the user. Adjudication on all disputes regarding the classification of help desk calls will be provided by IT Services Contract Management Team.
- The FM Supplier shall provide a comprehensive monthly statistical analysis of the Help Desk Calls as per the specification of the IT Services Contract Management Team

10. System and Application Access controls

Measures and procedures required to effectively control all aspects of system and application access.

10.1 Authorisation

- It is the responsibility of the Head of Service/system sponsor or their designated representative or an IS/IT Manager to authorise all requests for new users and amendments to user id and password set up, amendments, access rights/privileges and deletions. Authorisations must be confirmed in writing (or E-Mail).
- The System Sponsor is responsible for the regular review of all users and their access rights.

10.2 Terminal and Password Security

The following procedures shall be adhered to in respect of terminal and password security :

- Where possible passwords shall comprise a minimum of 6 characters to include at least one numeric.
- Users must take care to ensure that their passwords are kept private and secure and for their own use only.
- It is the users responsibility to ensure that they use passwords which would not be easily apparent to anyone wishing to facilitate unauthorised access.
- Terminals must not be left unattended when 'signed-on'.
- Passwords must be changed periodically and also comply with other adopted standards for passwords. Where applications provide, users will be forced to change their passwords on a 28/30 day cycle.
- Forgotten passwords will be reset only by the person authorised to issue passwords. Depending on the system or application in question, this may be a member of the Council's staff, an employee of the Council's FM Contract Supplier, or an officer nominated by the System Sponsor.
- Any user who suspects that the confidentiality of their password has been compromised in any way shall change that password at their earliest opportunity and immediately report the matter to their head of service.
- Each Service Unit must ensure that their computer users are aware of their responsibilities to follow good security practices in the selection and use of passwords.
- To facilitate Audit Trails, the inventory will contain full details of unique MAC addresses directly traceable to an individual's PC.
- Where appropriate, application time-out for inactivity can be applied per application at the discretion of the System Sponsor.
- Equipment which is located in any area deemed to present any risk of misuse of IT Services will have the additional security measure of a restricted access time where available. This will provide the ability to disable the terminal and/or facilities at certain times (ie. outside of normal office hours).

10.3 Network access control

The following procedures shall be adhered to in respect of Network access and control :

- Network firewall strategy
The Council maintains a secure, corporate Firewall facility which is applied to the permanent Internet 128Mb link and serves to protect the Council's Network, Applications and Data from unauthorised external access.
- Management and monitoring of user internet access and electronic mail activities shall be performed to identify any misuse of these facilities to support the Personnel and Management Services Internet utilisation guidelines.
- Access to the Network is strictly controlled by user id and password and users are only able to access those services and network directories which they have been authorised to use by the IT Services Team, their head of service.
- Access, external to the TDC Network, and access to TDC facilities via Modem links for such purposes as remote diagnostic links and/or access to

external, authorised application systems (such as the Council's bank) shall be the subject of strict control procedures and access verification in respect of their initial connection and subsequent use. All such modem installations shall be fully documented by the FM Supplier and shall be reviewed on a quarterly basis. Remote diagnostic links will only be used under session specific supervision and shall be disconnected and immobilised when not in use.

10.4 Monitoring access and use

- The IT FM Supplier is responsible for implementing adequate security measures to prevent unauthorised access to systems and applications and also to detect security breaches or attempted security breaches where they have occurred. All development User passwords will be secured and maintained to a standard agreed by the Council. All specifications for this area of responsibility are detailed in Schedule 2 of the IT Services Agreement.

11. Systems Development and Maintenance Standards

Security requirements of systems shall incorporate the following safeguards :-

- Control over operational software implementations/releases
- Protection of test data
- Formal change control procedures shall be operated
- Modifications to packages will be discouraged and strictly controlled
- Any new system development or modification to an existing system shall only be carried out with the appropriate authority of IT Sub-Committee, IT Services, Head of Service and/or System Sponsor.
- The Council's IT FM Supplier is responsible for the maintenance of all change control documentation, including the maintenance of hardware/software/application manuals, release version levels and test system environments.
- All proposed new development will include all of the following mandatory security features:
 - multi-level access controls
 - audit trails
 - backup/archive routines
 - formal change control procedures
 - maintenance of operational system documentation
 - all other specifications detailed within the IT Services Agreement in respect of the above shall apply.

12. Disaster Recovery

12.1 Data backup

In respect of both local and remote applications, backup of all Data and Software shall be taken and stored in a fire proof and off-site environment approved by the Council's IT Services, to ensure that Application Services can be:-

- recovered to the start of an Office Hours period in the event of a failure or serious error;
- recovered to the start of a session of batch updating in the event of a failure or serious error;
- recovered to a previous version of application or operating software in the event that a new version fails or introduces serious errors;
- recreated on another machine in the event of a disaster; complete backup of all data and software will be taken weekly and incremental backup of data will be taken daily and stored on a separate site from the location of the machine on which the data/software normally resides. The Council shall provide a centrally heated dry store facility at Clacton which can be utilised for this purpose;
- The ability to recreate Data and Software from backup media will be tested annually and after any major change in a manner that does not put the availability of Services at a risk;
- A full backup of all In-House software shall be taken weekly and stored off site (this off site store will be a damp proof and secure environment approved by the Council). Intermediate backup will be taken daily and stored on site in a fire proof environment. Full copies of system documentation will also be stored off site;
- In the event of a failure to a system, application, service or routine the IT FM Supplier shall not be allowed to modify data or parameter definition, without prior authorisation of the system sponsor. The Supplier shall confirm to the Council's IT Services Team where such action has been taken.

12.2 Disaster recovery

- The IT FM Supplier shall provide a Hot Start Disaster Recovery Service of all of The Council's mainframe Systems. In the event of a disaster, The IT FM Supplier shall manage the process of relocation and recovery of application systems to the disaster recovery facility.
- The Council requires all mainframe services to be available within 48 hours of the original disaster.

The Disaster Recovery Service will include:-

- The recovery and provision of The Council's Mainframe Systems at a Disaster Recovery facility, utilising the most recent backup securities available at that time.
- Disaster Recovery facilities for any other server or system operated from The Suppliers premises which is remote to The Council's nominated local premises.
- Access to those recovered systems for The Council's authorised system Users from their normal place of work.
- An annual rehearsal to allow the comprehensive testing of The Council's and the Supplier's Disaster Recovery plans.
- The Council's IT Services Team will liaise with the System Sponsors to arrange for End User testing of the Mainframe systems.

- It is The IT FM Supplier's responsibility to arrange for the necessary annual testing of this facility with the test plan being agreed in advance with The Council's Contract Management Team. Within two weeks of the testing being completed The IT Supplier shall provide a fully documented report on the test to The Council's Contract Management Team. The Council will require the entire process to be overseen/checked by its Internal Audit staff.
- The Council has a Cold Start Disaster Recovery service. The service provides The Council with a relocatable, air conditioned, powered, computer room for use in the event of a disaster to The Customer's Computer Room. The Supplier shall be responsible for the co-ordination, operation and management of this Coldstart Recovery Facilities in the event of a disaster.
- In the event of a disaster, The Supplier shall provide all possible assistance to The Council to facilitate the expedient recovery and reinstatement of IT Services and data.
- The Supplier shall, as part of the support to servers, undertake a recovery exercise for each network server on an annual basis. The Council will provide a suitable server for this purpose or authorise the use of an existing server to validate the recreation of application systems.

12.3 Fire and other Emergencies

- The employees or subcontractors of the Supplier will be expected to understand and comply with the Council's Fire alarm and Emergency procedures.
- The Council must be informed of any work being undertaken by the Supplier likely to effect fire precautions.
- The Supplier will ensure that there is a procedure in place to ensure that all its staff and visitors to the Supplier's staff can be accounted for in the event of an emergency.
- The Council will inform the Supplier of any Fire drills or emergency to the building housing the computer room. On these occasions the power to the computer room will not be disconnected, but staff must comply with the requirements of the drill.
- In the event of an emergency the Computer room power supply will be disconnected using the emergency cut off buttons located in the computer room.
- An inventory of all IT equipment maintained on behalf of the Council will be kept up to date and accessible at all times in the event of a fire.
- After office hours, and when the computer room is unoccupied, the Halon Fire detection system will be set to automatic.

13. Compliance With Legislation

To avoid breaches of statutory, criminal or civil obligations the following conditions shall be strictly adhered to :

13.1 Control of material and software

- Legal restrictions on the use of copyright material (**Copyright, Design and Patents Act**)

Only official licenced copies of software purchased or procured by the Council may be installed on any equipment used by the Council. Staff must consider the implications of copyright when copying, scanning or, in any other way, replicating information and/or software.

- Council software shall only be installed on fully authorised business machines.
- Regular audits of software and maintenance of software registers.
- All computer programs and data purchased, developed or rented for the Council, are for the sole use of providing facilities for the Council.
- Deliberate unauthorised access to, copying of, alteration of, destruction or interference with computer programs, data or equipment is expressly forbidden.

13.2 Data Protection

To ensure full compliance with all Data Protection legislation the following procedures will be strictly adhered to :

- all information held (electronic and manual files) relating to living individuals will be reviewed by the nominated Service Unit representative on a monthly basis to ensure that the Council's use of such data complies with the Data Protection Act principles and is in accordance with the purposes contained within the Corporate Data Protection Registration.
- all computer printouts containing personal or sensitive data are to be stored in suitable storage facilities so that the information is not available to unauthorised persons.
- staff must be aware of the need to ascertain that any person requesting data, (particularly over the telephone) is entitled to it, are who they say they are and that the data subject has given written permission for the information to be passed. If there is any doubt, information must not be given out until verification is received. Verify the validity of the request and the data subject's permission and then contact the person requesting the data.
- Service Units will provide confirmation of their monthly review of data to the IS Manager who will review requirements and arrange for the appropriate amendments/deletions/confirmations of register entries.
- compliance with data protection legislation.
- Data Protection information will be provided at all staff induction courses and guidance and advice provided to all managers and users.
- procedures for handling data subject access requests will be maintained and regularly reviewed.

13.3 Prevention of misuse of IT facilities

- The Council's IT Facilities will only be used for authorised business purposes. Guidance and advice will be provided to all managers and users.
- The Computer Misuse Act 1990 as amended, applies in full in respect of all use of TDC IT equipment and systems.
- The Security procedures detailed in this policy document will minimise any occurrence of the three criminal offences - unauthorised access, unauthorised access with intent to commit a further serious offence, and unauthorised modification of computer material detailed within this Act.

14. Data Utilisation Control and Media Handling

14.1 General

All data utilisation and media handling (including the disposal of data) must always be with due regard to the sensitivity of the data and current legislation.

14.1 Secure disposal

- any amendment, disclosure, destruction or operation involving data or programs belonging to the Council must be properly authorised and controlled.
- all disposal of printed data must be carried out using the Council's secure waste disposal procedures;
- all information held (electronic and manual files) relating to living individuals must be reviewed on a monthly basis to ensure that the data is both current, required and not excessive in relation to the purposes contained within the Corporate Data Protection Registration. Redundant information must be deleted/disposed of in a secure manner;
- waste computer printed output must be disposed of with due regard to its sensitivity. Confidential output must be shredded or destroyed. Individual sections are responsible for ensuring the required facilities are provided.

14.2 Network management

- The Supervisor/Administrator passwords will not be divulged to anyone other than authorised staff without the express written permission of The Contract Management Team.
- Any amendments to a server's configuration, including the addition of users or groups or the reorganisation of files, must be first authorised in writing by the appropriate System Sponsor.
- General users that are set up will, by default, only be given full access rights to their home directory and any designated public directories. They will also be given execute/ read access to any software provided for their use. Any extension to these rights must first be subject to authorisation by the System Sponsor or the Contract Management Team.
- Each server will be documented to include the following information as is already provided under current standards:

Software Version

Disc partitioning

Network Cards

Printer definitions

System Login Script

Group listing

Group members and Directory Assignments for each group

User full name, Login Script, and Directory Assignments for each User

Note - any changes will be historically recorded showing date of change and authorisation.

- The issue and administration of user login names and passwords will be carried out using the following procedures to ensure that:-

- Each User has a unique log-on and password for each Application Service, and each LAN that they have authority to use.
- Users are prompted and required to change their password for each Application Service and each LAN every 30 days (so long as the application/system software permits)
- Access to “Supervisor/Administrator” function on distributed servers will be strictly controlled by The Supplier under the direction of Contract Management Team. The Supervisor/Administrator password will be changed immediately following access by any third party support companies or in any event not less than once every month.

14.3 Media handling and security

Individual procedures for :

- the security of data, programs, output and equipment;
- authorised software and programs installation on the Council's equipment;
- inventory management and control of removable computer media;
- protection of system documentation from unauthorised access

Must be followed at all times.

14.4 Data and software exchange

- The Supplier shall comply (and shall ensure that its employees, servants, agents and Sub-contractors comply) with all reasonable instructions and/or guidelines produced by the Council from time to time for the handling and storage of Proprietary Information.
- The Supplier shall ensure that a Non-Disclosure Undertaking (in the form of Schedule 10 of the ITSA) is completed and signed for each of their employees or sub-contractors who, during the course of their employment, may obtain information belonging to The Customer or concerning The Customer and its business which is proprietary to The Customer and is supplied in confidence.
- Procedures for the security of media in transit are detailed within the ITSA.

15. Project Implementation and Review

Recognised project management methodology and software will be used to plan, manage and review all IT projects. All aspects of this security policy will be adhered to for each and every project.