Policy Document

IT Infrastructure Security Policy

[23/08/2011]

Document Control

Organisation	Redditch Borough Council
Title	IT Infrastructure Security Policy
Author	Mark Hanwell
Filename	IT Infrastructure Security Policy.doc
Owner	Mark Hanwell – ICT Transformation Manager
Subject	IT Infrastructure Security Policy
Protective Marking	Unclassified
Review date	23/08/2011

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Head of Business Transformation	Deborah Poole	23rd August 2011

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1 Policy Statement

There shall be no unauthorised access to either physical or electronic information within the custody of the Council.

Protection shall be afforded to:

- Sensitive paper records.
- IT equipment used to access electronic data.
- IT equipment used to access the Council network.

2 Purpose

The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council's information, in line with section A9 of ISO/IEC/27001.

In order to ensure the continued protection of the personal, confidential and RESTRICTED information that Redditch Borough Council holds and uses, and to comply with legislative requirements, information security best practice, and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Government Connect Secure Extranet (GCSx), access to Redditch Borough Council's information equipment and information must be protected.

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the Council's IT data centre. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. No service should fall below the baseline security standard level of protection required for their teams and locations.

3 Scope

All Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council with access to Redditch Borough Council's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Council's equipment and the information that they use or manipulate.

4 Definition

This policy applies to all users of the Council's owned or leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of information within the custody of the Council.

This policy should be applied whenever a user accesses Council information or information equipment. This policy applies to all locations where information within the custody of the Council or information processing equipment is stored, including remote sites.

5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

6 Applying the Policy

6.1 Secure Areas

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g. fire, flood, vandalism.

As an example, access to secure areas such as the data centre and IT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should challenge anyone not wearing a badge. Each department must ensure that doors and windows are properly secured.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A Council ICT employee must monitor all visitors accessing secure IT areas at all times.

Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by ICT, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately. Please also refer to the IT Access Policy and Human Resources Information Security Standards.

6.2 Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from Information Services.

All equipment must have a unique asset number allocated to it. This asset number should be recorded in the Departmental and the IS / IT inventories.

For portable computer devices please refer to the Remote Working Policy.

6.3 Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Network cables should be protected by conduit and where possible avoid routes through public areas.

6.4 Security of Equipment Off Premises

The use of equipment off-site must be formally approved by ICT. Equipment taken away from Redditch Borough Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted if carrying PROTECT or RESTRICTED information.
- Be password protected.
- Be adequately insured.

Further information can be found in the Removable Media Policy and Remote Working Policy.

Users should ensure, where necessary and required, that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the ICT Department and the Insurance Section (if applicable).

Staff should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act (please refer to the Legal Responsibilities Policy).

6.5 Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools. Equipment must be returned to ICT for data removal.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

6.6 Delivery and Receipt of Equipment into the Council

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied:

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.
- Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

6.7 Regular Audit

There should a duty to audit information security arrangements regularly to provide an independent appraisal and recommend security improvements where necessary.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Redditch Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or ICT.

8 Policy Governance

The following table identifies who within Redditch Borough Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Transformation Manager
Accountable	Head of Business Transformation
Consulted	Corporate Management Team
Informed	All Council Employees, All Temporary Staff, All Contractors etc

9 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Transformation Manager.

10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- IT Access Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Remote Working Policy.
- Removable Media Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.

11 Key Messages

- PROTECT or RESTRICTED information, and equipment used to store and process this information, must be **stored** securely.
- Keys to all secure areas housing ICT equipment and lockable IT cabinets are held centrally by ICT, as appropriate. Keys are not stored near these secure areas or lockable cabinets.
- All general computer equipment must be located in suitable physical locations.
- Desktop PCs should not have data stored on the local hard drive.

- Non-electronic information must be assigned an owner and a classification. PROTECT or RESTRICTED information must have appropriate information security controls in place to protect it.
- Staff should be aware of their responsibilities in regard to the Data Protection Act.
- Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.