# ICT Security Policy

## GUIDANCE


Bassetlaw
DISTRICT COUNCIL
— North Nottinghamshire —

# ICT Security Policy

**Introduction**

This policy applies to all of Bassetlaw District Council and A1 Housing employees, here after called The Authority's.

The Authority recognises its obligations to protect information from internal and external threats and recognises that effective information security management is critical in order to ensure the successful enablement of ICT and delivery of business functions and services. The Authority is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets.

The purpose of the ICT Security Policy is to minimise 'the authority', its customers, employees and partners from information security threats, whether internal or external, deliberate or accidental.

Information is to be considered to be any knowledge or data that has a value to The Authority and which is collected, processed, stored, communicated or received. It can be written, printed, stored electronically, transmitted by post or electronic means, shown on films, or spoken in conversation.

Security is considered to be the protection of information against unauthorised disclosure, transfer, modification, retention or destruction, whether accidental or intentional.

Staff are considered to be all permanent, temporary, casual, and sessional and seconded of The Authority, Councillors, Board Members, contracted third parties working for the Authority and working in partnership with The Authority, whether working on premises, from third party premises or from home.

**Purpose**

The Key issues addressed by the Security Policy are:

- Confidentiality of information – ensuring that information is accessible only to those authorised to have access.
- Integrity of Information – safeguarding the accuracy and completeness of information and processing methods, system assets are operating correctly according to specification and in the way the current user believes them to be operating.
- Availability – ensuring that authorised users have access to information and associated assets when required.
- Regulatory – ensuring The Authority meets its regulatory and legislative requirements

The Authority will provide a corporate information security function to introduce and maintain policy standard and to provide advice and guidance on their implementation.

Departments are required to ensure that the confidentiality, integrity, availability and regulatory requirements of all business systems are met.

It is also the aim to ensure that all employees, consultants and contractors are aware of the possible risks, to outline their responsibilities for security and to provide guidance to them so that they may act in a professional manner to protect the information.

This security policy has been produced in line with guidelines laid out in ISO 27002:2005, which provides detailed guidance on information security and the relevant sections of the Government's Security Policy Framework.

In order to protect business continuity and reduce the risk of business damage, this policy aims to minimise the impact from security incidents.

The Authority's policy aims to ensure that:

- Computer systems are properly assessed for security
- Confidentiality, integrity and availability are maintained
- Staff are aware of their responsibilities, roles and accountability
- Procedures to detect and resolve security breaches are in place.
- The Authority undertakes appropriate ICT security training for all staff

This is a statement of policy and as such does not address daily practices. These are covered separately in individual operating procedures and standards.

This Policy should be read in conjunction with its associated Policies and Guidelines

BDC & A1 ICT Anti-Virus Guidelines
BDC & A1 Portable Devices Policy
BDC & A1 Remote Access for Third Parties Policy
BDC & A1 Internet & Intranet Policy
BDC & A1 Email Policy
BDC & A1 Encryption Policy
BDC & A1 Classification Policy
Social Media Policy

**Development of specific ICT policies, procedures and guidelines**

The Authority is committed to the ongoing development and review of ICT policies, procedures and guidelines to manage the risk of emerging threats to its systems and services. This work will be co-ordinated by the ICT Information Governance Group AND Finance and Sub Committee (A1). A list of current supporting documents is included in Appendix A. New policies, procedures and guidelines are distributed to all stakeholders at the time of issue.

## Security Management

The Authority depends on its ICT infrastructure for the retrieval, sharing and dissemination of business critical data, and the conduct of its business. Failure to adhere to adequate security standards could result in the alteration, theft, destruction or loss of ability to process the data.

Some of the data stored by The Authority is of a confidential or sensitive nature. Should the data become compromised then The Authority could face legal action for failing to protect it adequately as required by the Data Protection Act 1998. Such action would considerably damage The Authority credibility and incur significant legal costs including the imposition on unlimited fines.

Loss or damage of important business assets such as computer contact databases could result in incorrect business decisions or the perpetration of fraud. A significant failure might also cause Bassetlaw District Council to breach its obligations under the PSN Government Connect Code of Connection, which would jeopardise the delivery of a number of critical services.

## Auditors

The Authority's policy, its implementation and systems will be subject to periodic review by both internal and external auditors, the recommendations from which will be implemented and monitored by the ICT Governance Group and A1 Finance and Organisational Health Sub-committee. Any major security incident is liable to be referred to the auditors for investigation.

## Responsibilities

### ICT Services

The overall responsibility for the ICT Security lies with ICT Strategic Manager who is responsible for the implementation of ICT security across the networks for The Authority.

A1 ICT Manager and BDC Information Security Manager are responsible for the ICT Security policy and ensuring staff are made aware of the said policy, they receive information security training and they adhere to the guidelines laid out.

Responsibilities include:

- Monitoring and reporting on the state of ICT Security within The Authority.
- Ensuring that the ICT Security Policy is implemented throughout The Authority.
- Developing and enforcing detailed procedures to maintain security.
- Ensuring compliance with relevant legislation
- Ensuring that The Authority's employees, Board and Councillors are aware of their responsibilities and accountability for ICT security
- Monitoring for actual and potential ICT security breaches
- The network for The Authority's is managed and controlled by ICT Services and will be reviewed as to the requirements and security.
- Ensure each system is allocated a system administrator.
- Training of staff in ICT Security
- Review this document wherever there may be a change of influencing circumstances
- Maintenance of an inventory for all hardware/ software procured by The Authority's

## Line Management

- Ensure that all current and future staff are instructed in their security responsibilities
- Ensure that all their staff using computer systems are trained in their use
- Ensure that no unauthorised staff are allowed to access any of the Authority's systems as such access could compromise data integrity.
- Determine which individuals are to be given authority to access specific computer systems. The level of access to specific systems should be on a job function basis rather than status.
- Implement procedures to minimise the organisation's exposure to fraud/theft/ disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas
- Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability
- Ensure that all staff are aware of The Authority's Employee Code of Conduct on potential personal conflicts of interest.
- Ensure that the relevant systems administrators and ICT are advised immediately about staff changes affecting computer access so that access may be withdrawn, deleted or amended.
- Ensure when an employee leaves the organisation all company assets, including corporate documents and ICT equipment are returned. A completed form detailing all ICT Equipment the employee has will be sent to HR. Upon receipt of returned equipment, these will be reconfigured and reissued.
- Where third party external subcontractors are used to process information, then either they must sign up to The Authority's security policies or must have their own equally stringent policies (approved by ICT Services) which their staff are signed up to.
- Avoid where possible the need for them and their staff to use information, particularly personal data, outside of The Authority's offices, thereby minimising the risk of loss of data.

## Staff, Board and Councillor Responsibilities

- Each staff, Board and Councillor is personally responsible for ensuring that no breaches of information and equipment security result from their actions.
- Each staff, Board and Councillor shall sign acceptance for all The Authority's ICT Policies.
- Staffs, Board and Councillors are responsible for ensuring that they do not leave their computer in a vulnerable state allowing others to access systems and data in their absence, by logging off or using a password protected screensaver.
- Each staff, Board and Councillor should declare any potential conflicts of interest as required by The Authority's Code of Conduct.
- All reasonable steps must be taken to minimise the risk of losing information, particularly personal data. Advice in the BDC & A1 Portable Devices Policy and BDC & A1 Remote Access Policy should be followed.
- Each computer user is personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions
- Users should ensure that they do not disclose their passwords or allow anyone else to work under their details
- Any breach in security should be reported using the ICT Security Breach policy guidelines

## System Administrators

Each system will be the responsibility of a specified system administrator whose responsibilities will include ensuring compliance with The Authority's ICT Security Policy, ensuring appropriate use of the equipment, supplier liaison, troubleshooting, fault reporting and maintenance.

- All of The Authority's systems will have at least two individuals with the expertise to administer the particular system
- System Administrators will be responsible to the ICT Strategic Manager for continued system security

## Individuals' Responsibilities

ALL users must report any action that appears to contravene the ICT security Policy, any breach of information security or any suspected weakness immediately to A1 ICT through the ICT Security Breach procedure. Users are NOT to attempt to exploit suspected weaknesses.


**Infrastructure Security**
It is the responsibility of The Authority's Infrastructure Architect and ICT support staff to maintain the operational security of the network. The network infrastructure referred to in this standard means: wire connections, wireless connections, virtual connections and all intermediate devices that support the flow of information around the network.

### User Authentication
The Authority's systems require a unique user identification and password to be entered before access to the systems will be granted.

Formal procedures will be used to control access to system. Each application for access should be requested from the line manager. This should be made prior to an employee commencing employment.

Access privileges will be modified/removed as appropriate, when an individual changes job or leaves through the use of the starters/leavers forms. It is the responsibility of the Line Manager to inform ICT Services Desk when employees access levels needs changing. HR and Finance will inform ICT Service Desk when a user starts/leaves employment at The Authority.

No individual will be given access to a live system unless properly trained and made aware of their security responsibilities. This will be done by the individual's line manager.

Users should keep their password secret and never disclose them.

Each user will have a unique login id to access their computer. Passwords will be alpha numeric and be at least 7 characters long containing at least one number. Passwords will last no more than 90 days. Passwords should not be used again for at least a 20 change cycle. Three login attempts will be allowed before the network is locked out.

### Secure Password Guidance
The Authority's systems require a unique user identification and password to be entered before access to the systems will be granted.

When creating passwords use of the following rules help to ensure a secure password is created.

Do:

- Make them a minimum of 8 digits long (the longer the better)
- Use at least 1 upper case Alphabetic eg SECURITY
- Use at least 1 lower case Alphabetic eg SECURITY
- Use at least 1 numeric eg sECUR1TY
- Use at least 1 special character eg sECUR1TY-
- Use more than 1 word eg sECUR1TY-NAME
- Use embedded symbols instead of letters eg s3CUR1TY-N@ME
- Use first letters of a phrase

Do not:

- Use an embedded space character
- Start your password with a numeric character
- Use personal information such as derivatives of your user ID, names of family members, maiden names, cars, license tags, telephone numbers, pets, birthdays, social security numbers, addresses, or hobbies
- Create new passwords that are substantially similar to ones you've previously used
- Write your password down
- Use your account name or any part of your full name
- Use adjacent keys on a keyboard eg "asdf"

## Network

All networked file servers/core networking equipment will always be located in secure areas with restricted access.

The Authority's ICT suite will be a high security area, housing its most important on site computers. An entry restriction and detection system will be incorporated to protect the suite.

Local Area Networking equipment and Wide Area Network terminating equipment will always be located in secure areas and/or lockable cabinets.

Unrestricted access to the central computer facilities will be confined to designated staff, whose job function requires access to that particular area/ equipment. Restricted access may be given to other staff by the ICT Strategic Manager where there is a specific job function need for such access.

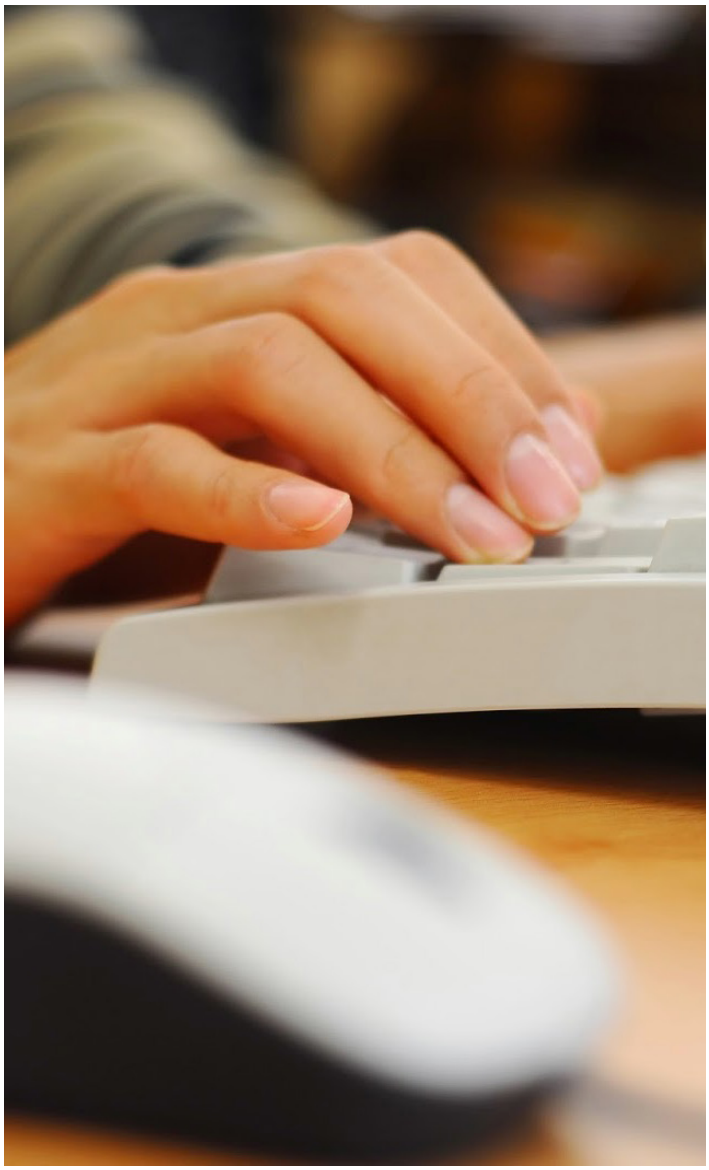
## Third Party Access

This section should be read in conjunction with the BDC & A1 IT Remote Access for Third Parties Policy.

No external agency will be given access to any of The Authority's networks unless that body has been formally authorised to have access. Each supplier requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives. All external activity will be monitored.

External agencies will only be allowed access to their own hardware/systems.

The Authority will control all external agencies' access to its systems by use of logins through the Corporate Portal for each approved access requirement. File uploads will not be allowed. Files can be sent to ICT Service Desk, then placed on the target server in an agreed location.



**Managed Computing Services**
It is the responsibility of The Authority, to ensure that adequate policies and procedures are in place to ensure compliance with ISO 27002:2005 in all aspects of the services provided through the SLA and all other externally sourced applications.

**Internet, Email and Social Media Access**
All users who are granted access to the Internet and email service however accessed must have signed to confirm that they have read and understood and are required to comply with all ICT Policies.

Social Media Access to sites (e.g. facebook, twitter, my space) is granted to staff, which needs to access for business use only. Users are only given access to these sites by ICT Service Desk and must have line manager's approval before access will be granted. Access to social media sites is strictly for business use only.

**Wireless**
All staff may use the wireless internet connection provided by The Authority for work purposes only after they have obtained 'wireless key'. All staff requesting access to the wireless network must obtain line managers approval. Request needs to be sent through to ICT Service Desk

Access by external organisations and customers will be through the use of a 'Wireless key' and will be granted by ICT Service Desk.

**Equipment Security**
All ICT and telecommunications equipment must be purchased through ICT Service Desk. Requests for equipment/software must have an appropriate business cases as required.

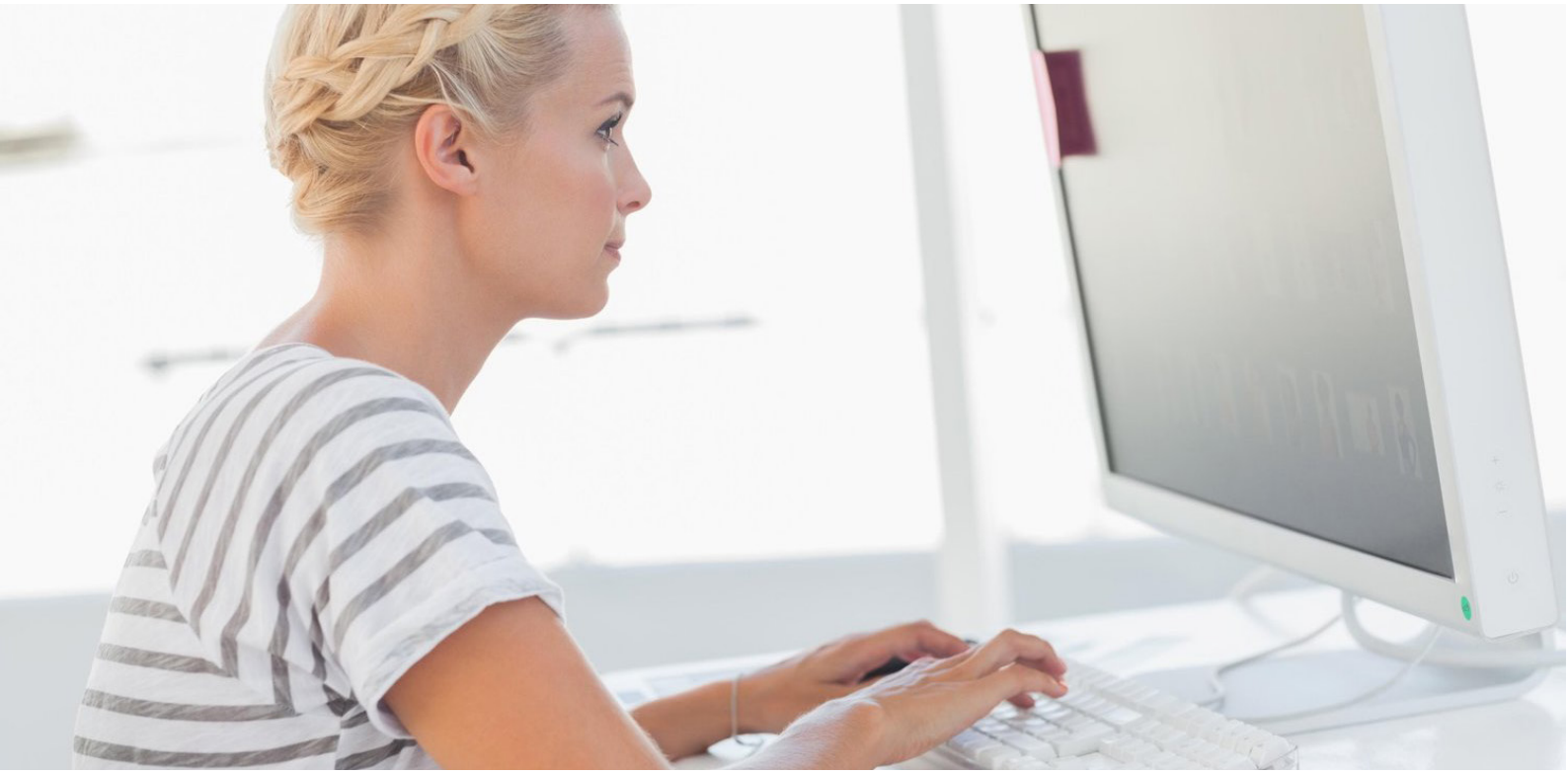
ICT and telecoms equipment should always be installed and sited by ICT Technical staff or the supplier in accordance with the manufacturer's specification if approved by the ICT Infrastructure Architect.

An up to date register of assets will be maintained by the ICT Service Desk. This will include the value, location, serial number. Each device and certain items of peripheral equipment will be tagged with a permanent label to identify it as The Authority's property.

Environmental controls will be installed to protect equipment. Such controls may trigger alarms if environmental problems occur. In such cases only authorised entry will be permitted.

Critical ICT equipment will be fitted with battery back-up to ensure that controlled shutdowns occur in the event of power loss. Such battery power should suffice for at least 30 minutes normal usage.

ICT equipment should utilise high integrity earth power circuits where these are available.



All cabling (electricity or communications) within buildings will be in conduit if surface mounted, otherwise within the framework of the building.

All central processing equipment including file servers, will be covered by third party maintenance agreements or by maintaining a 'hot spare'. The spare server will be kept within the server rack in the ICT Suite ready for use in the event of a total failure of one server.

All personal computers will be covered by a three year manufacturer's warranty. After the expiry of that warranty the computer will only be repaired if it is cost effective to do so at the discretion of the ICT Unit.

ICT equipment can be damaged by the accidental spillage of food or drink. In particular keyboards are most prone to this type of damage when cups of tea/coffee etc are placed close by and are then accidentally knocked over. The subsequent repair costs to any item of ICT equipment, (PC, laptop, printer, scanner etc) damaged in this way will not be covered by either the equipment warranty or The Authority's insurance and any costs will be charged against the service area budgets. Therefore it is highly recommended that food and drink is kept away from your ICT equipment.

Records of all faults to equipment will be maintained by ICT Service Desk.

Hard disks on any computer may contain sensitive/ confidential data. Removal off site of such disks represents a potential threat to The Authority. Each such case will be judged on its merits balancing the need versus the risk of breach of confidentiality agreements. Whenever possible the data and information should be overwritten or the hard disk destroyed. If the data is overwritten, it should be at least CESG IS5 basic standard.

Portable Devices are very vulnerable to theft, loss or unauthorised access, see the BDC & A1 Portable Devices Policy to ensure that such risks are minimised.

Portable devices must have a designated user responsible for the device. The designated user must comply with the BDC & A1 Portable Devices Policy and ensure that the policies are complied with.

Computer hardware disposal can only be authorised by the ICT Unit. The ICT Unit will ensure that data storage devices are purged of sensitive data before they are disposed of or completely destroyed. All equipment will be disposed of in compliance with WEEE (Waste Electrical and Electronic Equipment) regulations.

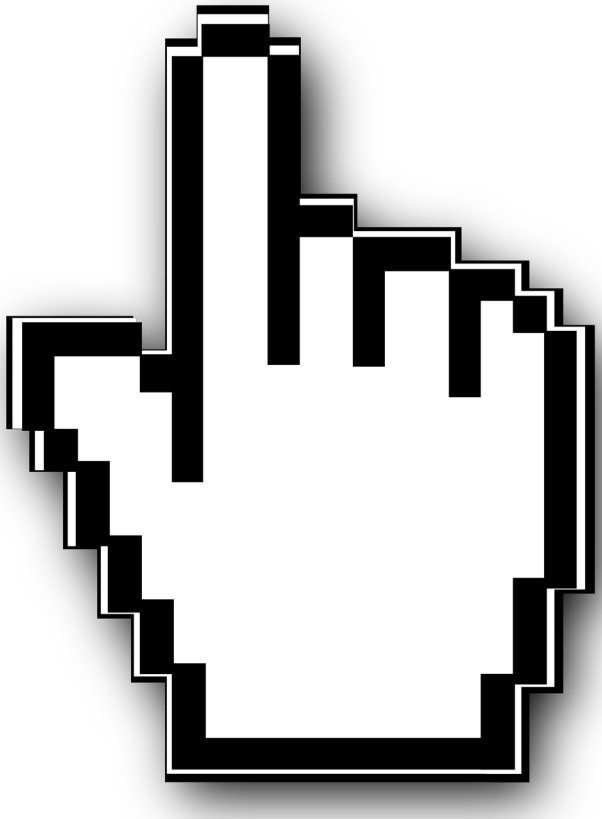
**Software**

Only use licensed copies of commercial software should be used. It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable for prosecution as well as disciplinary action. The Authority does not condone the possession of unlicensed software.

The Authority ICT Department will retain a copy of all licences for software that is provided by them. Software can only be loaded with the authorisation and assistance of ICT Services.

The Authority will require the use of specific general purpose packages (word processing, spreadsheet, databases, etc) to facilitate support and staff mobility.

Where The Authority recognises the need for specific specialised products, such products should be registered with the ICT services and be fully licensed.




**Data Validation**
Data accuracy is the direct responsibility of the person inputting the data supported by their line manager.

All systems will include validation processes at data input to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity.

Systems should report all errors together with a helpful reason for the rejection to facilitate correction.

Error correction should be done at the source of input as soon as it is detected. Such correction is increasingly important as systems are integrated and errors can be transmitted between systems.

Any loss or corruption of data should be reported to the relevant system manager and ICT service desk at once.

Data Protection principles should be adhered to when entering data, copies of the 8 principles along with a flowchart when being requested for information can be found on the Authority's Intranet.

A1 - http://intranet.a1housing.co.uk/data_protection_and_foi
BDC - http://intranet.bassetlaw.gov.uk/Default.aspx?page=1034#EIR

**Implementation of New Systems**
All system requests must be made through ICT Governance and Finance and subcommittee approval. These must be purchased through procurement procedures within ICT services.

**Housekeeping**
All central systems will have daily backup regimes formalised in the appropriate documentation. Backups will have a minimum of an 8 working day cycle before media is overwritten. Secure, fireproof storage will be used for all of the backup media held on site. Weekly backup media will be stored off site to protect against building loss.

Recovery contingency testing will be undertaken on a regular basis, at which time the viability of central systems' backups will be verified.

All users are advised that if they store data on their own PC hard drives, that data is NOT backed up by the ICT Department.

All users should not save confidential information on their hard drives.

All systems/application areas will be subject to a security review by systems administrators. The depth of review will be determined by the importance and size of the particular system.

Individual systems should be reviewed at least once every three years. Systems are liable to independent reviews by internal and external auditors.

Reviews will include:
Identification of assets of the system
Evaluation of potential threats
Assessment of likelihood of threats occurring
Identification of practical cost-effective counter measures
Implementation programme of counter measures

Each system review will include a formal report to the ICT Strategic Manager containing findings and recommendations

**Virus Control**

The Authority seeks to minimise the risks of computer viruses through education, good practice and procedures. Anti-Virus software will be installed on all The Authority's equipment, currently System Center 2012 – Endpoint Protection.

Users should report any virus detected or suspected on their PC's immediately to the ICT Services Desk.

**Disaster Recovery – The Authority**

The Authority recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business through tested disaster recovery plans.

The Authority recognises that ICT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

The main elements of this process will include:- Identification of critical systems.

- Identification and prioritisation of key users/ user areas.
- Agreement with users to identify disaster scenarios and what levels of disaster recovery are required.
- Identification of areas of greatest vulnerability based on risk assessment.
- Mitigation of risks by developing resilience
- Developing, documenting and testing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities.

Disaster recovery plans will cater for different levels of incident including :-

- Loss of key user area within a building
- Loss of a key building
- Loss of a key part of the computer network
- Loss of processing power

Disaster recovery plans will always include:-

- Emergency procedures covering immediate actions to be taken in response to an incident
- Fall back procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan
- Resumption procedures describing the actions to be taken to return to full normal service
- Testing procedures describing how the disaster recovery plan will be tested.

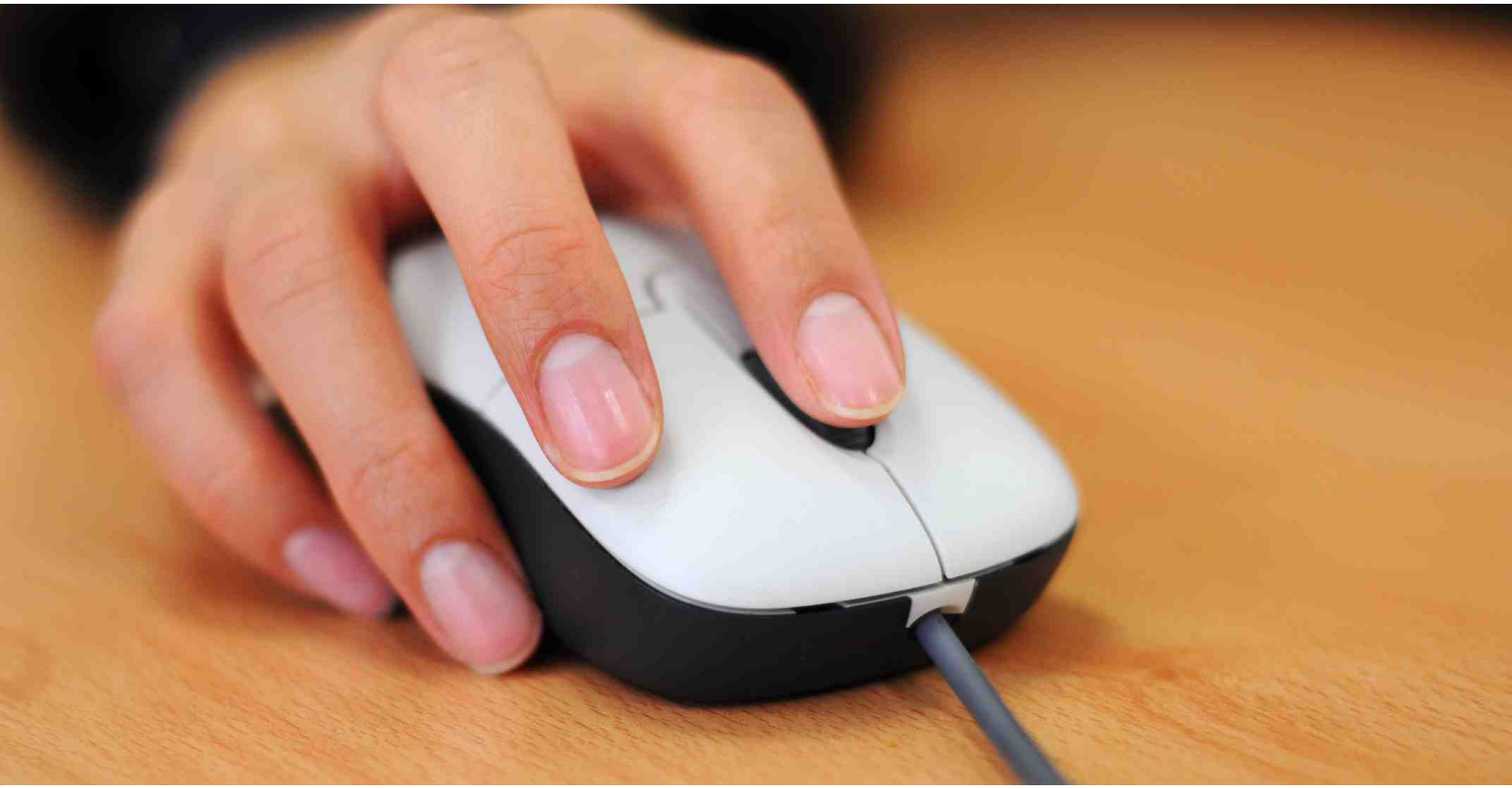
These procedures are meant to deal with the worst computer disaster The Authority could suffer, that of the destruction of the computer suite. This would lead to the invocation of disaster recovery.

In all cases the objective is to resume computer services although there may be excep¬tional reasons to delay. Users will be advised within 12 hours of the failure when computer services will be resumed and from which site.

The procedures have been devised by ICT Infrastructure Architect in consultation with users and suppliers of various software packages. Procedures and methods of implementation will vary from time to time. Users will be advised of new or revised procedures as soon as practicable.

System Administrators are required to create and maintain a Disaster Recovery Plan for systems they are responsible for. These plans will concentrate on actions and procedures to be followed by their staff/users in the event of loss of system. They will be used in conjunction with the ICT Disaster Recovery Plan and will contain detailed information for staff in service areas to re-instate normal working once the ICT Unit have provided a back-up system.

A copy of both sets of procedures should be kept in a secure place unlikely to be affected by fire, flood, explosion, etc.



**Incident Reporting**

A security incident is an event which may result in:-

- Degraded system integrity
- Loss of system availability
- Disclosure of personal information
- Disruption of activity
- Financial Loss
- Legal Action
- Unauthorised access to applications

All users are responsible for reporting any security breaches, whether this is information or equipment.

Further information regarding security breaches can be found in the BDC & A1 ICT Security Breach Policy.

**Discipline**

Any individual found deliberately contravening this policy or caught jeopardising the security of information that is the property of The Authority will be subject to The Authority's disciplinary procedure. In addition, in appropriate cases, individual employees may be subject separately to legal action by the relevant authorities, including the Information Commissioner.

**Appendix A**

List of ISMS Security – Policies

BDC & A1 Email Policy

BDC & A1 Encryption Policy

BDC & A1 ICT Anti-Virus Guidelines

BDC & A1 Security Breach Policy

BDC & A1 Information Sharing Protocol

BDC & A1 Internet and Intranet Policy

BDC & A1 ICT Patch Management Policy

BDC & A1 Remote Access for Third Parties Policy

BDC & A1 Portable Devices Policy

BDC & A1 Portable Equipment request sheet

BDC & A1 Portable Equipment Acceptable Use Guidelines

# Contact us


01909 533 533


www.bassetlaw.gov.uk


customer.services@bassetlaw.gov.uk


Text us on 07797 800 573


Find us on Facebook - BassetlawDC


Twitter @BassetlawDC


Visit us at:

Retford One Stop Shop
17B The Square, Retford DN22 6DB

Worksop One Stop Shop
Queens Buildings, Potter Street, Worksop S80 2AH

All offices are open: Monday to Friday 9:00am to 5:00pm

If you need any help communicating with us or understanding any of our documents, please contact us on 01909 533 533.

We can arrange for a copy of this document in large print, audiotape, Braille or for a Language Line interpreter to help you.

Bassetlaw
DISTRICT COUNCIL
North Nottinghamshire