Car Crash Salvage Information Security Management System Policy

bsi.

...making excellence a habit.™

Car Crash Salvage – Case Study

Company Profile

Car Crash Salvage – for the purpose of this case study will now be known as CC Salvage. This business has been around since 1950 and was originally a vehicle dismantling company. The company progressed into vehicle salvage in 1965. CC Salvage is the UK's largest independent company of its type. It has 3 locations, but with 4 sites. These are: Head Office & Canvey Island site, servicing the South East, Nottingham site servicing the Midlands and the Teesside site servicing the North & Scotland. The company employs 64 staff in total. The company has two distinct relationships, the first being with the insurance companies, where it provides the management of recovery, storage and then disposal dependant on the categories below.

Has the capacity to process 500k vehicles per annum. The types of vehicles are: all emergency service vehicles, all types of motorcycles, HGV, agriculture machinery and vehicles, caravans/mobile homes, camper vans, high value cars and all other motor vehicles. The company provides a full salvage service to the insurance industry. This includes the pick-up, storage, purchase and then auction on their website.

The vehicles are segregated into four different categories, which are: A, B, C & D.

Category A – destruction only, Category B – salvage for spares only, Category C – high damage, but repairable and Category D – low damage and repairable.

Annual Turnover for Car Crash Salvage – £150m with 20% profit

MG Transport Profile

MG Transport provides drivers and logistics support to CC Salvage for the pick-up and delivery from the pick-up point to the appropriate site. As instructed by CC Salvage (CCS) and Insurance Companies. The company has available up to fifty drivers and 10 admin staff, across all the CCS sites. All transport vehicles are owned by CCS, but are maintained and managed by MG Transport. This function was originally managed by CCS until 2002, when MG Transport (MGT) was established as an independent organisation. MG Transport is a key supplier to CCS.

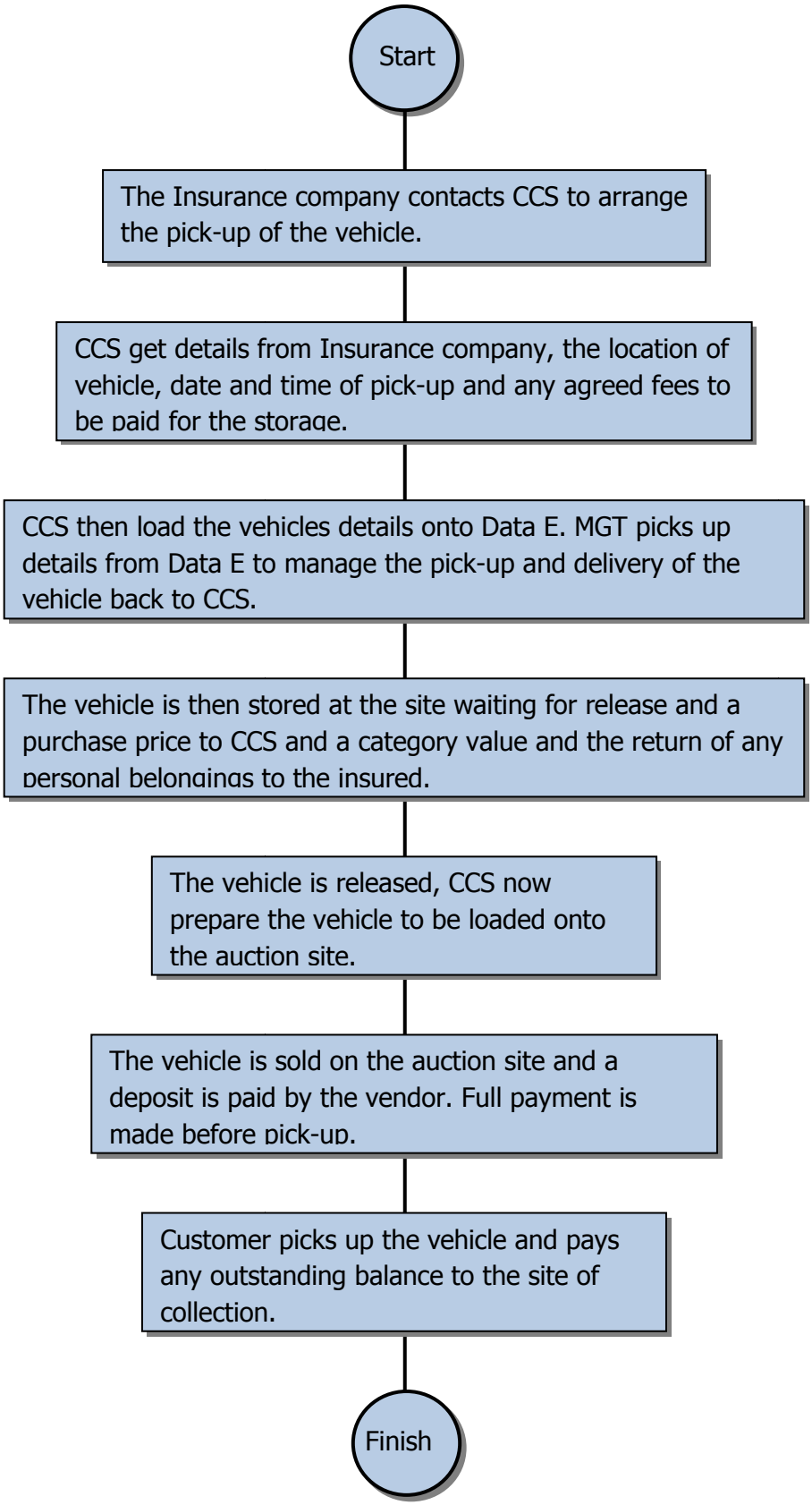
MGT share facilities and systems with CCS and have a very close working relationship with each other. MGT have their own management systems to deal with their drivers and to facilitate the day to day running of the company. They also have other clients.

1st Ondemand Profile

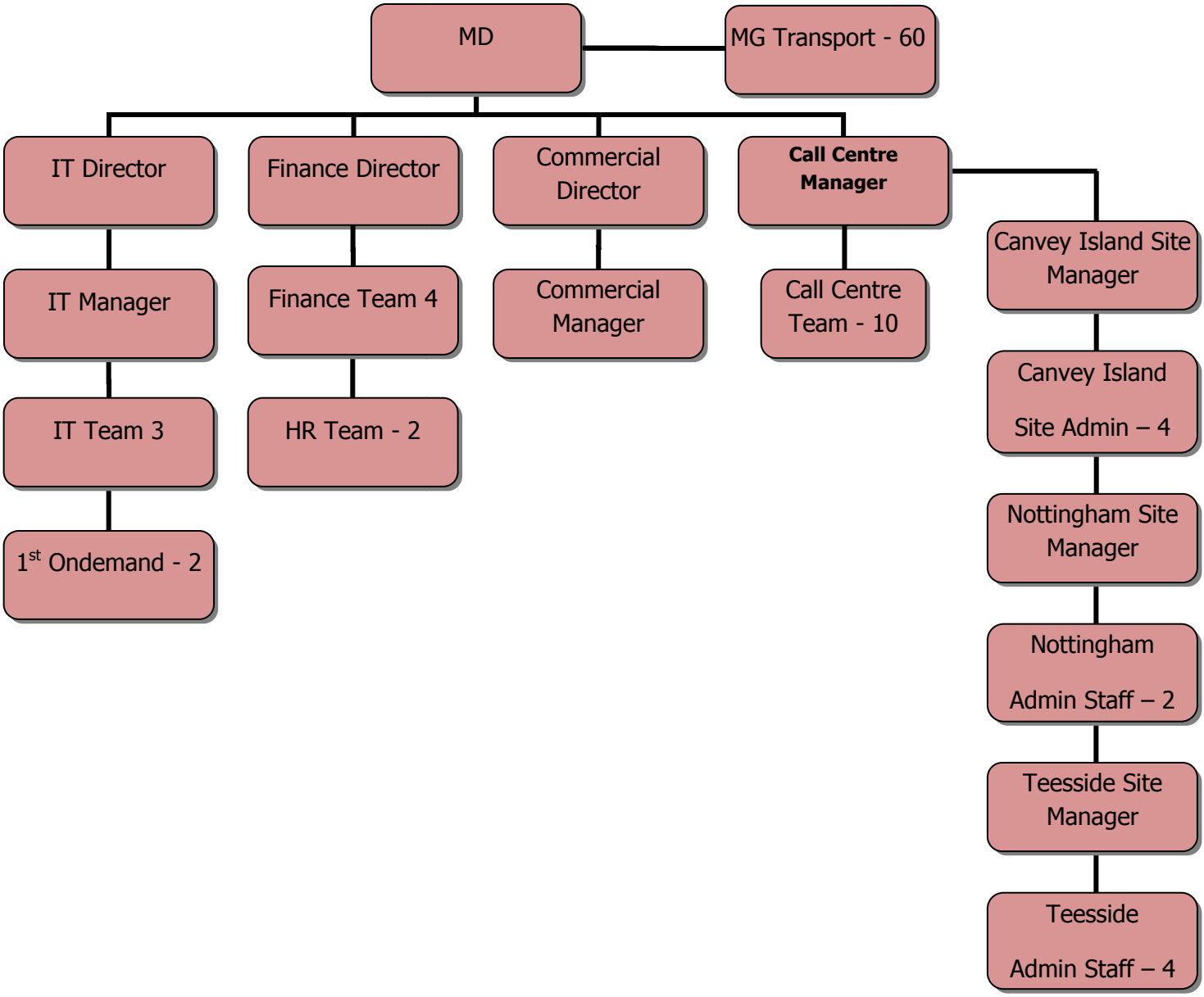
1st Ondemand are a software and website development company, who developed the auction website for CCS. They also have a number of clients in the health sector where they have built bespoke software solutions. In 2004 CCS bought out 1st Ondemand as they were seen as an integral part of CCS service provision (on-line auction system).

The company has 2 employees, who work from home. They spend their time providing continuous support to the health sector business and continuous support/development of the on-line auction website and any IT/development as required. The business turns over £3m per annum.

Car Crash Salvage – End to End High Level Process



Car Crash Salvage – Organisational Chart



Business Scope

Top management commitment of the introduction of an Information Security Management System within Car Crash Salvage Ltd for the provision to salvage all types of vehicles across the UK. Mainly including the North, Scotland, Midlands, South and South East. All sites included: Canvey Island, Nottingham and Teesside. Exclusions to scope are MG Transport and 1st Ondemand.

Drivers and Interested Parties for the ISMS

To have in place an ISMS will give CCS competitive edge over our competitors and will demonstrate world class status to all of our potential customers, including business and public sectors. Will secure the long term growth of CCS and secure the future of all of our employees. ISMS will ensure we put processes and procedures in place to make us more efficient, effective, health & safety, environmental and business continuity focused. Interested parties will be our customers, suppliers, local authorities and the police. Car Crash Salvage has no shareholders and is in the enviable position of having no bank debt and is a cash rich company. The budget set aside for the ISMS implementation programme was £100k. Resources required were external consultant, IT director and the IT manager.

Site Profiles

Head office located on Canvey Island. At HQ is all the board of directors, finance team, HR, call centre team, IT team and 2 MGT staff, but excluding 1st Ondemand. Located around HQ are a number of factories on a small industrial site. HQ has 2 contract cleaners, that clean daily. The site also holds 3 main frame servers and business contracts, employment records and all business processes are held on site. The site sits 8ft below sea level. Canvey Island has a sea defence system in place, which was built after the 1955 floods. The island sits in the middle of the Thames estuary. The physical site security is a reception desk, a camera system and the building is fully alarmed. There is parking for approximately 20 cars. The building is detached from any other surrounding property.

Canvey processing site is located approx. 1 mile from HQ. It is a 30 acre site, which has a perimeter fence and only has one neighbouring site, which is a Petro-Chemical site. Within 200 yards of the 2 sites is a housing estate, a local bistro pub. This CCS site is the main processing site for the south and south east. On the site itself a shared office, which locates CCS office staff and a sectioned off area for customer collection & payment. The rear of the building is used for MGT and their staff. There is a large parking area for CCS's HGV transport vehicles. The second building is a large pre-fabricated facility for storage of high value vehicles. This is again fully secure with alarms and cameras. This site has strategically placed cameras and sensors around the area. Viewing and pick-up are held 3 times per week, Mon, Weds & Fri. On entering each site, there is a security office, where customers or visitors are required to report into. They are then directed to the front office, for either collection or to view a vehicle they wish to bid on (at all times they will be accompanied by CCS staff).

Teeside is located on a 30 acre industrial estate. There is a chemical site nearby. This site employs a site manager, 4 admin staff and 8 yard staff. Teesside site works in the same way as the Canvey site.

Nottingham is located on a 12 acre site within a housing estate. The Nottingham site has no Heavy Goods Vehicles assigned to there. This site employs a site manager, 2 admin staff and 6 yard staff. Nottingham site works in the same way as the Canvey site.

The Information Security Management System Policy.

...making excellence a habit.™

Document Control

Version:	3
Date:	26th November 2011
Author(s):	Olivier Burrows, Steve Thorpe
Distribution:	All Car Crash Salvage Staff
Review Date:	26th November 2012

1 Information Security Management System Policy Statement

1.1 Policy

- The purpose of the Policy is to **protect Car Crash Salvage's (CCS) information assets from all threats**, whether internal or external, deliberate or accidental.
- CCS Information Strategy & Policy Group has approved the Information Security Management System Policy
- It is the policy of CCS to ensure that:
- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Regulatory and legislative requirements will be met
- Information Security Training will be provided
- All breaches of Information Security, actual or suspected, will be reported and investigated
- Standards will be produced to support the policy. These include virus controls and passwords
- Business requirements for the availability of information and information systems will be met
- The Head of Information Compliance & Policy has direct responsibility for maintaining the policy and providing advice and guidance on its implementation
- All Managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff
- It is the responsibility of each employee to adhere to the Information Security Management System Policy

Signed: _____

Title:_____ Date:_____

(The Head of Information Compliance & Policy will review this policy, usually 1 year from the date signed)

2 Introduction

This Policy has been developed to protect all systems within CCS to an adequate level from events which may jeopardise CCS activity. These events will include accidents as well as behaviour deliberately designed to cause difficulties.

2.1 Policy Statement

CCS will seek to ensure that the confidentiality, integrity and availability of its information are maintained by implementing best practice to minimise risk.

2.2 Need for a Security Policy

The data stored in manual and electronic systems used by CCS represents an extremely valuable asset. The increasing reliance on information technology for the delivery of services makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion in addition to paper based records.

The increasing need to transmit information across networks of computers renders the data more vulnerable to accidental or deliberates unauthorised modification or disclosure.

2.3 Legal Requirements

Some aspects of information security are governed by legislation, the most notable U.K. Acts are:

- The Data Protection Act (1998)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Human Rights Act (2000)

For a more detailed explanation of each of the above see Appendix A.

2.4 Purpose and Scope of the Policy

The purpose of security in any information system, computer installation or network is to preserve an **appropriate** level of the following:-

Confidentiality the prevention of the unauthorised disclosure of information

Integrity the prevention of the unauthorised amendment or deletion of information

Availability the prevention of the unauthorised withholding of information or resources

The level of security required in a particular system will depend upon the risks associated with the system, the data held on the system and the working environment of the system.

This policy applies to all information held in both manual and electronic form.

2.5 Who is affected by the Policy

The Policy applies to all employees of CCS. It also applies to contractors and visitors, not employed by CCS but engaged to work with or who have access to CCS information, e.g. computer maintenance contractors.

2.6 Where the Policy Applies

The Policy applies to all locations from which CCS systems are accessed (including home use or other remote use). Where there are links to enable non-CCS organisations (to have access to CCS information, CCS must confirm the security policies they operate meet our security requirements or the risk is understood and mitigated.

The Policy applies to all systems and all information whether academic, administrative or any other.

2.7 Security Policy Objectives

- To ensure all staff have a proper awareness and concern for computer systems security and an adequate appreciation of their responsibility for information security.
- To ensure all contractors and their employees have a proper awareness and concern for security of CCS information.
- To provide a framework giving guidance for the establishment of standards, procedures and computer facilities for implementing computer systems security.
- To meet the general objectives of ISO 27001 Code of Practice for Information Systems Security.
- To specify CCS responsibilities.
- To ensure all staff have an awareness of the Data Protection Act (1998) and its implications.
- To ensure that all staff have an awareness of the Computer Misuse Act 1990.
- To ensure that all staff is aware of their accountability and that they are aware that failure to comply with the Information Security Management System Policy is a disciplinary offence which may include action up to and including summary dismissal. Any action taken will conform to the appropriate CCS Human Resource policies.

2.8 Review and Audit

The I.T. Department is responsible for regular review of the Policy in the light of changing circumstances. The review will occur annually or when there are significant changes. CCS Internal Audit Office has a brief to ensure that the Policy is appropriate for the protection of CCS interests.

3 Acceptable Use

All use of computer systems will comply with the The I.T. Department Acceptable Use Policy. Acceptable use is defined as use for the purposes of:

1. Administration and management of CCS business
2. Development work and communication associated with the above
3. Consultancy work contracted to CCS
4. Reasonable use of computer facilities for correspondence, where not connected with any commercial activity, is at present regarded as acceptable.

It is CCS policy that all use of the facilities shall be lawful, honest and decent, and shall have regard to the rights and sensitivities of other people.

4 Security Management and Responsibilities

4.1 Objective

To ensure that staff are aware of security risks and their responsibilities to minimise the threats.

Rationale – Information Security is a shared responsibility. Confidentiality, integrity and availability of information could be compromised due to a breach of security (which could be accidental or malicious) occurring at any point in the information flow.

4.2 Car Crash Salvage (CCS)

CCS policy is to accept all reasonable obligations in respect of information security and to protect its information resources by implementing best practices which achieve an effective balance between cost and risk.

4.3 I.T. Department Security Support

The I.T. Department is responsible for providing help and guidance on all matters relating to information security BUT ultimately data owners are responsible for ensuring compliance with the above policy statements and that the systems under their control have an appropriate level of security.

4.4 Data Owner

Each Departmental or Branch Manager is responsible for their own departmental computer system where such exists. Key responsibilities include:

- Data subject enquiry procedures (as required by the Data Protection Act 1998).
- To ensure, in liaison with The I.T. department, the software license to use the system is accurate, available and purchased according to financial regulations
- Agreeing details of who can access what information, how and when, according to the particular classification of the information.
- Agreeing and understanding in general how the system is maintained in an effective and controlled manner.
- Ensuring that staff immediately reports any violations or misuse of the system to them. The Data owner will then liaise with The I.T. Department as necessary.
- Application training and password control.
- Media and equipment disposal procedures in liaison with the I.T. Department.

Systems which are operated throughout CCS should also have a designated Data Owner or be owned by The I.T. Department direct.

The I.T. Department will offer advice to data owners as to how they can manage their responsibilities. With existing systems, advice is available to help data owners meet their responsibility in complying with the Information Security Management System Policy. With new and proposed systems, advice must be sought at the planning and development phase to ensure systems will meet the security policy requirements before purchase and installation.

4.5 Systems Development

All system developments must comply with the I.T. Strategy for CCS. All system developments must include security issues in their consideration of new developments, seeking guidance from the I.T. Department where appropriate.

4.6 Management Responsibilities

It is the responsibility of managers to ensure the following, with respect to their staff:

a) All staff should be instructed in their security responsibilities.

b) Staff using computer systems/media must be trained in their use

c) Staff must not be able to gain unauthorised access to any of CCS IT systems or manual data which would compromise data integrity.

d) Managers should determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.

e) Managers should implement procedures to minimise CCS exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas.

f) Current documentation must be maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable.

g) All staff should be aware of the confidentiality clauses in their contract of employment and/or the Employee Handbook whichever applies.

h) Managers must ensure that The I.T. Department is advised immediately about staff changes affecting computer access (e.g. job function changes leaving department or organisation) so that passwords may be withdrawn or deleted as appropriate.

i) Managers must ensure that all contractors undertaking work for CCS have signed confidentiality (non-disclosure) undertakings.

j) Managers should ensure that all staff have access to and have read CCS Information Security Management System Policy.

4.7 Staff & Temporary Staff Responsibilities

a) Each employee and temporary is responsible for ensuring that no breaches of information security result from their actions.

b) Each employee and temporary is responsible for reporting any breach, or suspected breach of security.

4.8 System Managers

a) Job descriptions for system managers will include specific reference to the security role and responsibility of the post

b) The IT systems within CCS should have a minimum of two, preferably three individuals with the expertise to manage or administer such a system.

c) System Managers will be responsible to the Head of Information Compliance & Policy for continued system security.

d) System Managers are responsible for promptly issuing user accounts

e) System Managers must ensure that only those persons who are authorised to have access are provided with that capability.

5 Enabling the flow of information

5.1 Objective

To enable the efficient flow of information without compromising its integrity and confidentiality

5.2 Sharing data/information with other organisations

CCS works with partner organisations which all have a legitimate role to play in delivering service. Partners, in this context, are taken to be, but not limited to:

- industrial partners
- companies, and other agencies who may have legitimate need of access to information.

A formal Information Sharing Protocol will, in time, be developed, which will make the standards of information protection control explicit, rather than implicit.

5.3 Sharing data/information with non-partner organisations

CCS receives regular requests for personal data. Organisations requesting such information include:

- The Police
- Insurance companies
- Government bodies
- Banks

Whilst such requests may be legitimate, CCS will ensure the use of such information is not abused and is in line with the Data Protection Act 1998, by applying the following principles when considering the release of the information to non-partner organisations:

- Information will not be released without the consent of the individual concerned

This principle may be waived in certain conditions (e.g. as a result of a court order, or where this information is required by law) but only after authorisation has been obtained.

5.4 Objective

To ensure that CCS uses electronic, postal and verbal communications appropriately.

5.5 Network Security

CCS will engage a third-party specialist to routinely review network security.

5.6 Telephone Security

CCS management will ensure that staff is aware of the importance of checking the credentials of all callers requesting personal or otherwise sensitive information.

5.7 Email (see also specific Email section)

Email should be used according to the conditions described here. The use of email may be monitored.

5.8 Internet

Staff should be aware of, and abide by the Acceptable Use Policy(Section 3). Use of the Internet may be monitored.

5.9 Fax security

CCS management shall ensure that fax communications are protected at all times and that faxes containing personal or sensitive information are sent, and received in a secure manner.

5.10 Verbal Communications

CCS management will ensure that all staff are advised and regularly reminded of their obligation to respect the privacy of staff. This means holding conversations discreetly and with due regard to the sensitivity of the subject under discussion.

6 Risk Management

6.1 Objective

To identify and counter possible threats to CCS information security and standards.

An assessment of all risks will be made for each information system to ensure that it is secured appropriately and cost effectively. Information systems within CCS face many risks which a Security Policy can reduce or eradicate:

6.1.1 Business Continuity

The risks of disruption to day to day business are reduced by informing staff about contingency procedures, backup and safekeeping of records.

6.1.2 Protection for Employees and Records

The security policy will ensure better protection of confidential information from unauthorised access. Well protected records are less likely to fall into the wrong hands or be misused. Standardised procedures also protect honest employees because they know what is expected of them, therefore protecting their integrity if a serious incident occurs.

6.1.3 High Data Quality

Good security measures often function as preventative internal controls, they help eliminate mistakes. Error correction is often the most time consuming of all manual processes and reducing errors frees staff to concentrate on developments and improvements.

6.1.4 Risk of Computer Crime

Following a strict security policy ensures staffs closes the loopholes in working practices, which makes life more difficult for thieves attempting to remove computer equipment.

6.1.5 Risk from viruses

Viruses are one of the greatest threats to computer systems.

PC viruses become easier to avoid with staff aware of the risks with unlicensed software or bringing data/software from outside CCS. Anti-virus measures reduce the risks of damage to the network.

The I.T. department centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from The I.T. department if any remedial action is necessary.

Further guidance is contained in section 26 of this document.

7 Awareness

Objective

The objective of Information Security is to ensure business continuity and minimise damage by preventing and minimising the impact of security incidents.

Notes:

1. Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on any digital media or spoken in conversation or over the telephone.
2. The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.
3. Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.
4. This applies to record keeping and most controls will already be in place. It includes the requirements of legislation such as the Data Protection Act.

Managers are responsible for ensuring that all staff are aware of and adhere to this Information Security Management System Policy. The I.T. department will ensure that Security is included in all Computer User Training. Departmental managers are responsible for ensuring their staff attends these awareness sessions.

Awareness material about Information Security will be made available as part of CCS intranet and will be accessible from http://192.168.0.23.

In order to maintain CCS information security and integrity, departmental managers must view Information Security training as essential.

8 Confidentiality Agreements

CCS will continue to adopt comprehensive policies and procedures to ensure the secure handling of personal information within all information environments such as complying with the Data Protection Act 1998.

Computer system users should be aware of their confidentiality (non-disclosure) undertaking which will either be part of the contract of employment or the acceptance of the conditions of the Employee Handbook dependent upon staff level and authority. This applies particularly to staff with access to sensitive data or systems. Before signing for their Handbook or signing their Contract of Employment, each employee should have the conditions carefully explained by the Manager or Director or other such officer delegated by them.

Agency staff and third party users not already covered by an existing contract (containing the confidentiality undertaking) should be required to sign a Confidentiality Agreement prior to employment/registration. These Confidentiality

Agreements should be reviewed when there are changes to terms of contract, particularly when systems are upgraded or contracts are due to end.

9 Business Continuity

Departmental management will be aware of the provisions of the Business Continuity Plan with respect to their own department and the BCP provisions for company business continuity or disaster recovery.

The I.T. department will be responsible for the technical aspects of all contingency plans and can provide advice on aspects of system data "catch up". They will maintain the BCP to ensure that all critical systems can be restored as quickly as possible if necessary.

9.1 Objective

To be able to restore computer facilities to maintain essential business activities following a major failure or disaster.

9.2 Need for effective plans

CCS 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.

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

CCS requires tried and tested disaster recovery plans for its computing facilities to be maintained.

9.3 Planning process

The main elements of this process will include:-

- identification of critical computer 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

9.4 Planning framework

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

- loss of a key user area within a building
- loss of a key building
- loss of a key operational area
- loss of a key part of a computer network
- loss of a computer's processing power
- loss of key staff

Disaster recovery plans will always include:-

- emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel)
- fallback 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
- evidence of regular and adequate testing of Disaster Recovery Plans

10 Equipment and Software Registers

10.1 Objectives

To identify the location and authorised use of CCS computer assets

10.2 Equipment Inventory

An inventory of all computer and equipment and software will be maintained. It is the responsibility of each department manager or their named representative to detail each item of computer related equipment and software purchased, or disposed of, to the The I.T. department. This department will keep a copy of the inventory and will periodically audit software that is installed. This policy will enable differences over time to be seen and then accounted for.

10.3 Software Register

An up to date register of all proprietary software will be maintained to ensure that CCS is aware of its assets and that licence conditions are followed. This register will normally be maintained by The I.T. department. System managers are responsible for informing The I.T. department about the purchase of any software and that this purchase conforms to CCS financial regulations.

11 Access control to secure areas

11.1 Objective

To minimise the threat to CCS computer systems through damage or interference.

11.2 Physical security

All networked file servers/central network equipment will be located in secure areas with restricted access.

Local network equipment/file servers and network equipment will be located in restricted access areas and if appropriate within locked cabinets.

11.3 Entry controls

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 where there is a specific job function need for such access.

Authenticated representatives of third party support agencies will only be given access through specific authorisation.

Regular reviews of who can access these secure areas should be undertaken.

12 Security of Third Party Access

12.1 Objective

To enable CCS to control external access to its systems.

12.2 Access control

No access will be given to any of CCS networks without formal authority. All non CCS personnel or companies will be required to sign security and confidentiality agreements with CCS before such authority is granted.

CCS will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

CCS will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

All third parties and any outsourced operations will be liable to the same level of confidentiality as CCS Staff

13 User Access Control

13.1 Objective

To control individual's access to systems to that required by their job function.

13.2 Access to Systems

Staff and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment, conditions of contract for contractors and student access agreements should have a non disclosure clause, which means that in the event of accidental unauthorised access to information, the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

13.3 Eligibility

The following are eligible to register as users:

1. any person holding a contract of employment with CCS;
2. any person holding an honorary position recognised by CCS;
3. Any Insurance company personnel or Engineer that we have a relationship with.

With the exception of access to material intended for the general public, use of information systems and networks shall be restricted to registered users.

13.4 Registering users

Formal procedures will be used to control access to systems. An authorised manager must countersign each application for access.

Access privileges will be modified/removed - as appropriate - when an individual changes job/leaves.

Each application for access should be countersigned by the manager against the rules agreed by The I.T. Department.

13.5 User password management

A password is confidential authentication information composed of a string of characters used to access computer systems.

Passwords must be kept confidential. Passwords are the responsibility of individual users; they must not be used by anyone else without specific management approval. The giving of an authorised password to someone unauthorised in order to gain access to an information system may be a disciplinary offence. All system managers will ensure their systems enforce password changes at intervals agreed by the Company Management.

It is best practice for passwords to be at least 6 characters in length. They should be a mix of characters including numerics. It is good practice to use 'screensaver' passwords in multiple occupancy offices, and essential in public areas. Passwords should be changed at intervals agreed by the Company Management and new systems should be built to encompass this.

No staff should be given access to a live system unless properly trained and made aware of their security responsibilities.

13.6 Staff leaving CCS employment

When a member of staff leaves the employment of CCS, their email account record is ended as part of the termination action carried out by HR. CCS regularly check accounts based on this information and ensure that all email accounts for members of staff no longer with CCS are terminated.

Prior to an employee leaving, or to a change of duties, line managers should ensure that:

- the employee is informed in writing that he/she continues to be bound by their signed confidentiality agreement
- passwords are removed or changed to deny access
- relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists
- supervisors passwords allocated to the individual should be removed and consideration given to changing higher level passwords, to which they have access
- reception staff and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitors pass
- where appropriate, staff working out notice are assigned to non-sensitive tasks, or are appropriately monitored
- departmental property is returned

Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment. Once an employee has left, it can be impossible to enforce security disciplines, even through legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

13.6 Staff leaving CCS employment (contd.)

System managers will delete or disable all identification codes and passwords relating to members of staff who leave the employment of CCS on their last working day. Prior to leaving, the employee's manager should ensure that all PC files of continuing interest to the business of CCS are transferred to another user before the member of staff leaves. It is good practice for an 'exit' interview to be held during which the manager notes all the systems to which the member of staff had access and Informs the relevant system managers of the leaving date. Special care needs to be taken when access personnel data and commercially sensitive and financial data is involved.

Managers must ensure that staff leaving CCS employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to CCS information and equipment.

In certain circumstances where exiting staff retain a formal relationship with CCS after they leave they may be provided with access to an email account after they have left the employment of CCS for a limited time.

In certain circumstances to be evaluated on a case by case basis researchers may be provided with access to an email account after they have left the employment of CCS for a limited time.

13.7 Visitors and Contractors

All visitors to Departments should have official identification issued by CCS and their arrival and departure times recorded. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation. Managers are responsible for informing The I.T. department when temporary staff leaves.

There is a requirement for System managers to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. The I.T. department will advise on the most suitable control.

13.8 The Internet

Staff who wish to use CCS computers and CCS telephone equipment for Internet services must have their 'connection' approved by The I.T. department.. The issuing of a user account would normally constitute approval.

14 Housekeeping

14.1 Objective

To maintain the integrity and availability of computer assets.

14.2 Data Backup

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Should information be held on a PC hard drive the PC "owner" is responsible for backups.

Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

The I.T. department and all other systems managers should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this backup. A cyclical system, whereby several generations of backup are kept, is recommended.

Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location.

Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes.

Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back up is taken and by using the back-up data in regular tests of the contingency plan.

Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data.

This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

14.3 Equipment, Media and Data Disposal

If a machine has ever been used to process personal data as defined under the Data Protection Act (1998) or "in confidence" data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software.

Therefore, disposal should only be arranged through the I.T. department who will arrange for disks to be wiped.

15. Software and Information Protection

15.1 Objective

To comply with the law on licensed products and minimise risk of computer viruses.

15.2 Licensed software

All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

The loading and use of unlicensed software on CCS computing equipment is NOT allowed. All staff must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. CCS monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under CCS Disciplinary Policy.

15.3 Unauthorised Software.

CCS will only permit authorised software to be installed on its PCs. Approval will be via The I.T. department.

CCS will require the use of specific general purpose packages (e.g., word-processing, spreadsheets, databases) to facilitate support and staff mobility. Non approved packages should be phased out as soon as practicable unless there is a definable business use.

Where CCS recognises the need for specific specialised PC products, such products should be registered with The I.T. department and be fully licensed.

Software packages must comply with and not compromise CCS security standards.

Computers owned by CCS are only to be used for the work of CCS. The copying of leisure software on to computing equipment owned by CCS is not allowed. Copying of leisure software may result in disciplinary action under CCS Disciplinary Procedure. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by The I.T. department staff or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

15.4 Virus control

CCS seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas.

Users should report any viruses detected/suspected on their machines immediately to The I.T. department. No newly acquired disks from whatever source are to be loaded unless they have previously been virus checked by a locally installed virus checking package.

Users must be aware of the risk of viruses from the internet, including email. If in doubt about any data received please contact the The I.T. department for anti-virus advice.

15.5 Time-out procedures

Inactive terminals should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also close both application and network sessions.

A high risk area might be a public or external area outside the control of CCS security management. The time-out delay should reflect the security risks of the area.

Users should log off terminals or PCs when leaving them unattended for any extended period, e,g. over 1 hour or when the PC area will itself be unattended or insecure.

For high risk applications, connection time restriction should be considered. Limiting the period during which terminal connection to IT services are allowed reduces the window of opportunity for unauthorised access.

16 Equipment Security

16.1 Objective

To protect IT equipment against loss or damage and avoid interruption to business activity

16.2 Equipment sitting and protection

IT equipment must always be installed and sited in accordance with the manufacturer's specification. Equipment must always be installed by, or with the permission of The I.T. department.

Where appropriate, environmental controls will be installed, to protect central or key equipment. Such controls will trigger alarms if environmental problems occur. In such cases where equipment is sited in a secure area, only authorised entry will be permitted.

16.3 Power supplies

Where appropriate CCS sites will have either UPS or generator backup to the mains electricity supply for key equipment.

16.4 Network Security

It is the responsibility of the Head of IT to ensure that access rights and control of traffic on all CCS networks are correctly maintained. Access rights to networked applications will be controlled by system managers. The Head of IT will control access to personal data held on networked servers.

Each System Manager has a responsibility for keeping the Head of IT informed of their requirements. This will include the number and names of users, their access requirements in terms of times and locations, the activities requiring network support and the needs of the support contractors.

System Managers must keep the Head of IT informed of new users requiring access and those users who no longer need access either through changing jobs or leaving the employment of CCS.

It is the responsibility of the Head of IT to ensure that data communications to remote networks and computing facilities do not compromise the security of CCS systems.

All communications cabling will be arranged by the I.T. department and cannot be authorised without their involvement.

16.5 Portable & Hand-held Computing Equipment

Equipment, data or software must not be taken off-site by staff without documented management authorisation. (Management may provide authorisation on a 'once only' basis as long as it is subject to regular review)

Portable computers must have appropriate access protection, for example passwords and encryption and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptop and handheld equipment when leaving an office unattended. When travelling, the high incidence of car theft makes it inadvisable to leave in cars or take them into vulnerable areas.

To preserve the integrity of data, frequent transfers must be maintained between portable units and the main CCS system. The portable unit must be maintained regularly and batteries recharged regularly.

Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off CCS property. The equipment should only be used by CCS staff to which it is issued. All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to CCS.

Users of this equipment must pay particular attention to the protection of, personnel data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may make arrangements for basic training in the use of a portable computer.

Users of portable equipment away from CCS premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage. Staff who use portable computers belonging to CCS must use them solely for business purposes otherwise there may be a personal Tax/National Insurance liability.

16.7 System Documentation

All systems should be adequately documented by the System manager and should be kept up to date so that it matches the state of the system at all times. In this context system documentation relates to the configuration, processes etc. of CCS systems and not material which would otherwise be in the public domain.

System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

Distribution of system documentation should be formally authorised by the system manager.

System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.

17 Incident Management

The The I.T. department Emergency response procedures have been defined. These categorise emergencies into three categories:

- Physical Security
- External failure
- Systems security

The associated documentation and process chart details the actions to be taken to restore or to rectify the situation and the creation of a working party.

All users must contact the I.T. Department if there are aware of, or suspect a security breach.

18 Electronic Mail (Email) Policy

18.1 Policy

CCS provides employees with access to a variety of information technology systems and electronic communication media including Email for the pursuance of CCS business.

18.2 Email

18.3 Care in drafting Emails

Users are responsible for drafting all emails carefully, taking into account any form of discrimination, harassment, CCS representation, and defamation of Data Protection issues.

Staff Emails are a form of corporate communication and therefore should be drafted with the same care as letters. Before sending proof read to make sure your message is understandable and appropriate. Do not send sensitive or emotional emails. If you are angry re-read it after you have calmed down. Never draft an email solely using CAPITALS – use normal sentence case.

Users should be careful when replying to emails previously sent to a group.

18.4 Viruses and Attachments

Employees are responsible for NOT opening any attachment received without prior knowledge of its contents and safety.

18.5 Information Confidentiality

Email is an insecure method of communication with content easily copied, forwarded or archived. Sensitive data should not be sent by this means.

18.6 Intent to enforce and monitor

CCS reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via email blocking software may be used to block and read any email on CCS network at any time by CCS. CCS is committed to ensuring that any monitoring is undertaken with reference to the privacy of the user and with regard to the Data Protection Act, the Regulation of Investigatory Powers Act, the Lawful Business Regulations and the Human Rights Act.

18.7 Retention and Purging

Deletion of old emails must be managed by each individual user, keeping in mind storage levels, archival levels, contractual evidence and legal discovery issues.

18.8 Email best practice

18.9 Junk mail

Email should not be sent to large numbers of people unless you are sure that it is directly relevant to their job. Sending unsolicited mail to many users ('spamming') is wasteful of user time and can disrupt the service, via performance delays, for other users.

18.10 Very large files

Sending of large files should be avoided where possible. The use of appropriately licensed compression software (e.g. *.zip files) is advised. Extremely large files should be sent by means other than email.

18.11 Mail Storms

Avoid 'Mail Storms' – long discussions sent to a distribution list – consider verbal communication.

19 Staff, Financial and Corporate Record Storage & Transportation

19.1 Objective

To identify and counter possible threats to CCS Records and determine protocols for their storage and transportation.

19.2 Storage

19.2.1 Offices

All Staff, Financial and Corporate Records should be stored in a secure area and not left in an unattended, unlocked room. They should only be retained for the minimum length of time that they are absolutely required.

19.3 Elsewhere

All other areas where Records are stored should follow general the best practice guidelines of:

- Stored in a secure area
- Not left unattended
- Not kept for longer than necessary

19.4 Transportation

Where it is necessary to transport Records around CCS sites, the individual is responsible for ensuring their security. Records should not be left unattended at any time. When being transported by car records should be stored in a concealed area.

19.5 Responsibility

All CCS Staff who use, or come into contact with confidential records are individually responsible for their safekeeping. Staff should be aware of their contractual and legal confidentiality obligations.

20. Home working Information Security Standards

20.1 Objective

To provide staff with information about the standards that should be used when they are working at home using computers (privately or CCS owned) and data. This applies equally to electronic and paper-based data. This can be a confusing area and it is necessary to ensure that staff is informed and confident that they are doing the right thing.

Today's technology allows a number of options about the way we work. CCS will continually study these options and develop appropriate protocols.

20.2 Use of person-identifiable data at home

20.2.1 Authorisation to remove data files

Formal written authorisation by the appropriate Data Owner is required before person-identifiable data files can be taken home. Each Data Owner must inform the I.T. Department of all staff who regularly work with information at home.

20.2.2 Transfer of personal data files

Person identifiable data files must not be sent via email to a user's home mail box. The Information (Data Protection) Commissioner has advised that Internet mail is not secure and should not be used to transmit

confidential information.

20.2.3 Protecting data files

All confidential electronic files used at home, where possible, need to be protected at least by file level password control.

20.3 Use of Privately owned Computers at Home

General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore you must use care when transferring data between your home PC and CCS network. All home PCs which are used for the manipulation of CCS data must have a current virus checker.

20.4 Transportation of data or confidential documents

You should take reasonable care to minimise that risk of theft or damage, IT equipment must be transported in a clean, secure environment. During transfer of equipment between home and work you should keep the equipment out of sight and not leave it unattended at any time. Computer equipment or manual data must not be left in your car overnight.

20.5 Storage of equipment

You should take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

20.6 Storage of confidential data or reports

You should secure confidential data or reports that you are not actively using in the most secure area of your home.

21 Appendix A: Legal Requirements

21.1 Data Protection Act (UK) 1998

The purpose of the Act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied rather than those of the people or Universities who control and use personal data. The Act applies to both computerised and paper records.

CCS will comply with the registration requirements of the Data Protection Act 1998 and any replacement European Union (EU) law. This Act requires that appropriate security measures will be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

The Act is based on eight principles stating that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subjects rights
- Secure
- Not transferred to other countries without adequate protection

21.2 Copyright, Designs and Patents Act 1988

These Act states that it is illegal to copy and use software without the copyright owners consent or the appropriate licence to prove the software was legally acquired. Each manager is responsible for ensuring that all items of software in their department are either purchased through, or sanctioned by, the Information Systems Department.

All software purchased will have an appropriate licence agreement which may or may not be a site-wide licence. CCS, through the Information Systems Department will carry out periodic spot checks to ensure compliance with Copyright Law. Any infringement or breach of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under CCS Disciplinary Policy.

21.3 Computer Misuse Act 1990

This Act states that it is a criminal offence to **attempt** to gain access to computer information for which you have no authorisation. If it is suspected that any unauthorised access is made to a computer system then disciplinary action may be taken under CCS Disciplinary Policy.

On ending their employment or work for CCS, employees and contractors must not disclose information which was confidential.

21.4 Freedom of Information Act (2000)

The Freedom of Information Act gives everyone a legal right to see information held by public authorities. (CCS is classified as a Public Authority). The aim is to open up public organisations and to make them more accountable to the electorate.

The Act complements the Data Protection Act 1998; if a disclosure is permitted under the Data Protection Act then the Freedom of Information Act gives the right of access to it.

21.5 ISO 27001

ISO17799 is the International Standard on Information Security Management initially developed by the British Standards Institute and the Department of Trade and Industry with the co-operation of various private and public sector organisations, including Healthcare. There are two parts to the application of this standard:

Part 1 is a "Code of Practice for Information Security Management" and provides a comprehensive set of security objectives and control requirements for those organisations seeking to demonstrate compliance with ISO 27001.

Part 2 is a specification for Information Security Management, suitable for certification of an organisation's information security system.

They provide a set of key controls considered necessary to comply with the standard and detailed guidance to assist the implementation of Information Security. The objective is to provide organisations with "a common basis for providing information security and to enable information to be shared between organisations", which is particularly significant with the increasing exchange of electronic information.

21.6 Human Rights Act

The part of the Act most relevant to Information Security refers to Article 8 of the European Convention on Human Rights. Personal data is part of an individuals "private life" and as such they have the right to have such information treated in the strictest confidence

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

22 Antivirus Guidelines

1. What is a Virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There is currently something like 60-75,000 known viruses and worms[1] - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

2. What does CCS I.T. department do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, security officers, and anti-virus software. The best efforts of administrators and security experts are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

3. Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, and unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden for to install them. If such programs are claimed to be some form of anti-virus or anti-Trojan[2] utility, there is a high risk that they are actually in some way malicious!

4. Treat All Attachments with Caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know; don't assume they must be OK because you trust the sender. Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply. However, one recent virus sends out an email telling you that a "safe" attachment is on the way, and then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

- If they come from someone you don't know, who has no legitimate reason to send them to you.
- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice" or "I love you!").
- If the attachment has a filename extension that indicates a program file (such as those listed below).
- If it has a filename with a "double extension", like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a

text file or JPEG (graphics) file.

In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

5. Avoid Unnecessary Macros

If Word or Excel warn you that a document you're in the process of opening contains macros[3], regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros. Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

6. Be Cautious With Encrypted Files

It is CCS policy not to use encrypted files in its general systems. Encrypted files are unlikely to have come from a company source and may contain hidden executable or malicious files. Occurrences should be reported to the I.T. Department immediately.

7. Suspicious Filename Extensions

The following is a list of filename extensions that indicate an executable[4] program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort. Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

[1] A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

[2] In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

[3] In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

[4] An executable is a file that contains a program. It is a particular kind of file that is capable of being executed or run as a program in the computer. In a Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe.

.BAT	.CHM	.CMD	.COM	.DLL	.DOC	.DOT
.EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
.SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

8. Report It!

If you think that you may have received a virus - ***Report It!***

23 Glossary & Abbreviations

For the purposes of this document the following definitions apply:

Access controls - the prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

Accountability - The property that will enable the originator of any action to be identified.

Asset owner- individual or organisation having responsibility for specified information assets and for the maintain of appropriate security measures

Audit trail - Data collected and potentially used to facilitate any reconstruction of events in a system

Authentication- Corroboration of the origin and correctness of any part of the system

Authorisation- The granting of rights which includes the granting of access based on access rights

Availability- Information is delivered to the right person, when it is needed

Confidentiality- Data access is confined to those with specified authority to view the data

Data Owner- The person who internal to CCS determines the purpose for which the information is to be used.

Data user- Data user means a person who holds data. A person holds data if:

> The data forms part of a collection of data processed or intended to be processed by or on behalf if that person
>
> *And*
>
> That person either along or jointly or in common with other persons controls the contents and use of the data comprised in the collection
>
> *And*
>
> The data are in the form in which they have been or are intended to be processed and with a view to being further so processed on a subsequent occasion
>
> *[Data Protection Act (1998)]*

Degauss- To remove unwanted magnetic fields and effects from magnetic disks, take or read/write heads

Denial of service - The prevention of authorised access to resources or the delaying of time critical operations

Impact - The embarrassment, harm, and financial loss, legal or other damage which could occur in consequence of a particular security breach

Information Security - Protection of information for confidentiality, integrity and availability

Integrity - All system assets are operating correctly according to specification and in the way that the current user believes them to be operating

IT - Information Technology

Password - confidential authentication information composed of a string of characters

PC - Personal Computer

Personal Data - Data consisting of information which relates to a living individual who can be identified form that information (or from that and other information in possession of the Data User), including any expression of opinion about the individual but not any indication of the intentions of the Data User in respect of that individual

> [Data Protection Act (1998)]

Person Identifiable Data - Any of the following items:

Surname, forename, initials, address, postcode, date of birth, other dates, sex, NI number, ethnic group, and occupation

Recovery- Restoration of a system to a desired date following a failure in the operation of the system

Risk - The likelihood of occurrence of a particular threat, with the degree of vulnerability to that threat and the potential consequence of that impact if the threat occurs

Risk assessment - Comprehensive concept for defining and assessing the potential impact of threats, and vulnerabilities of, system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security counter measures

Security breach - Any event that has, or could have, resulted in loss to Holding and Barnes assets, or action that is in breach of Holding and Barnes security procedures

Security Policy - A statement of the set of rules, measures and procedures that determine the physical, procedural and logical security controls imposed on the management, distribution and protection of assets and information

Sensitivity - A measure of importance assigned to information to denote its confidentiality

System Manager - The person charged with the technical administration of the computer system.

System Owner - The person who determines the purpose(s) for which the system is to be used.

Threat - An action or event which might prejudice security

Vulnerability - A security weakness

24 Associated policies, procedures, standards and guidance notes

This Information Security Management System Policy must be complied with and acted upon by all members of staff, contractors and others authorised to do so, in conjunction with, and under the terms of the following CCS policies:

- Disciplinary Policy and Procedures

25 References

This policy is based on the guidelines given in the following reference documents. However staff with specific responsibility for Information Security may wish to refer to the source documents.

1 The Data Protection Act (1998)

2 ISO27001

bsi.

...making excellence a habit.™

CCS Assets:

Head Office:

People:

Senior Management Team: 4 Directors.
Call Centre Team: 1 Manager, 2 Team leaders, 8 Call centre operators
Hr Team: 2
Finance Team: 4
MGT team: 2
IT team: 1 Manager 2 IT team 1 working from home.

Information Assets:

Job Description - Paper and Electronic – 19
Business Contracts – Paper -100
Process maps – Electronic – 100
Contract of Employment – Paper – 64
Insurance Documents – Paper – 100 (Including Vehicle, Property, Equipment and Employee)
HR Documents: Employee Information – Paper and Electronic including current and pass employees contracts of employment, salaries - 120 documents.
E-mails
Business Plans – Plans Growth, Financial reports.
Project Plans
Letter Heads.

To Protect Company Image & Reputation:

Company Brand – CCS
Quality of Service
Customer Confidence
New Business
Media
Client Confidentiality
Business Continuity

Software for all sites:

MS Office Professional – 30 copies
Data-Es – Vehicle processing software built by CCS IT 40 copies including 10 copies for MGT.
Auction Website- Access to all CCS Members – Use 2 Server 1 being back up.

E-mail System software and Internet Access.
Firewalls and antivirus software.
Security monitoring software for security cameras

Physical Assets:

26 – Computers, key board and muse.
6 – Laptops
6 – Printers
12- I Pads
12 – I Phones
27- Desks
27- Chairs
30 – Ink cartages
2- Digital Cameras
4- Security Cameras
1- Security Camera monitoring unit.
27- Phones
1- Telephone system
4- Security Waste Bins
20- Memory sticks

Assorted office equipment paper, pens etc.
6 – Company Cars.
70 – HGV – 10 used for spares 10 back up and 50 used daily by MGT daily.
6- Servers 1 located at the MD for additional back up as well as iron Mountain.

Services:

Gas
Water
Electricity
Telephone lines – managed by BT – all sites
Security System Service for all sites
Security Waste disposal for all sites one per month – all sites
6- Contract cleaner for all sites
Iron Mountain Back up – for all sites
Wi-Fi – for all site provided by BT
UPS- 40 mins of runtime if power outage.

Canvey Site:

People:

Site Manager - 1
Team Leader – 2
Admin Staff – 3
Yard Staff – 6
Security Officer-1
MGT Staff – 5

Information Assets:

Log Books – 500 +
Insured Personnel effects
Cash receipt
Customer records
Site processes

All software is provided by head office and loaded onto the machines by the IT team.

Physical Assets:

6 – Computers, key board and muse.
1 – Laptops
2 – Printers
1- I Pads
1 – I Phones
6- Desks
6- Chairs
10 – Ink cartages
2- Digital Cameras
10- Security Cameras
1- Security Camera monitoring unit.
6- Phones
4- Security Waste Bins
2- Memory sticks
Supply of Safety boots and hard hats
Cash - £1000- 50,000 held on 3 days of the week

Assorted office equipment paper, pens including high visual jackets, hard hats and gloves.

1 – Company Cars.

3- Diesel – Electric Forklift trucks
4- Jet washers
2- Full tool kits
3- 4x4 cars to transport customer around the site- these are all ex- salvage vehicles

Services:

Gas
Water
Electricity
Telephone lines – managed by BT – all sites
WI-FI

Teesside Site:

People:

Site Manager - 1
Team Leader – 2
Admin Staff – 3
Yard Staff – 6
Security Officer-1
MGT Staff – 5

Information Assets:

Log Books – 500 +
Insured Personnel effects
Cash receipt
Customer records
Site processes

All software is provided by head office and loaded onto the machines by the IT team.

Physical Assets:

6 – Computers, key board and muse.
1 – Laptops
2 – Printers
1- I Pads

1 – I Phones
6- Desks
6- Chairs
10 – Ink cartages
2- Digital Cameras
10- Security Cameras
1- Security Camera monitoring unit.
6- Phones
4- Security Waste Bins
2- Memory sticks
Supply of Safety boots and hard hats
Cash - £1000- 50,000 held on 3 days of the week

Assorted office equipment paper, pens including high visual jackets, hard hats and gloves.

1 – Company Cars.

3- Diesel – Electric Forklift trucks
4- Jet washers
2- Full tool kits
3- 4x4 cars to transport customer around the site- these are all ex- salvage vehicles

Services:

Gas
Water
Electricity
Telephone lines – managed by BT – all sites
WI-FI

Nottingham Site:

People:

Site Manager - 1
Team Leader – 2
Admin Staff – 1
Yard Staff – 4
Security Officer-1
MGT Staff – 2

Information Assets:

Log Books – 500 +
Insured Personnel effects
Cash receipt
Customer records
Site processes

All software is provided by head office and loaded onto the machines by the IT team.

Physical Assets:

6 – Computers, key board and muse.
1 – Laptops
2 – Printers
1- I Pads
1 – I Phones
6- Desks
6- Chairs
10 – Ink cartages
2- Digital Cameras
10- Security Cameras
1- Security Camera monitoring unit.
6- Phones
4- Security Waste Bins
2- Memory sticks
Supply of Safety boots and hard hats
Cash - £1000- 50,000 held on 3 days of the week

Assorted office equipment paper, pens including high visual jackets, hard hats and gloves.

1 – Company Cars.

3- Diesel – Electric Forklift trucks
4- Jet washers
2- Full tool kits
3- 4x4 cars to transport customer around the site- these are all ex- salvage vehicles

Services:
Gas
Water
Electricity
Telephone lines – managed by BT – all sites

WI-FI

CCS & 1st Ondemand – Documentation Control Procedure

...making excellence a habit.™

OBJECTIVE OF THIS DOCUMENT

The purpose of this document is to define the controls for creating, storing, using and disposing of paper company documents, classified because of their business, financial or personal content or key to business security. Creation, storage and disposal facilities are made available in all company departments.

Digital documents are created and handled on the appropriately protected system disks.

CLASSIFICATION OF DOCUMENTS

CCS confidential documents, normally marked with the main 'Confidential' heading, are classified in three groups:

Classification	Access	Description
1 CCS Employees Only	CCS employees	Not to be taken outside CCS premises without managerial permission and not to be discussed with non-CCS employees including past employees
2 Need to Know Basis	CCS Officers & assigned staff	CCS Officers, assigned CCS staff or Contract employees with a specific need to access the information in the document. These documents can be distributed to persons outside the CCS Group with the express permission of a director or employee of the Group.
3 Directors Only	CCS Directors	Only available to the directors of the group.

CREATING DOCUMENTS

CCS documents are created using office software via the system facilities made available to employees.

Where there is no requirement for classification of a document, i.e. it does not contain financial, personal or business sensitive information, then an ordinary blank document template may be used.

Where there is a classification requirement, normally defined to the employee by the Officer or Manager responsible or being created by an Officer or Manager, templates are available to create a document with the appropriate headers and footers containing the classification.

DOCUMENTATION UPDATES

Documents being held on the system which need updating are either updated by IT or authorised staff or printed by the assigned employee, marked in pen with the required update clearly identified and returned to the IT department, who then make the changes and update the documentation on line.

Notification that master documents have been updated will be via an e-mail or a telephone call from the IT department to appropriate personnel.

Paper copies of all CCS/1st Interactive key documents are in folders (Process Map, Training Matrix etc.) and are controlled via a Master Document Control List. Once an online document has been changed it is printed, placed into the relevant document folder and the document control list is updated to reflect the date of the new document. A Document Control list for each folder is kept at the front of the folder.

REQUIREMENT TO UPDATE

Any CCS employee has the facility to have incorrect or outdated documents corrected or brought up to date.

When an employee finds a document which is incorrect, the employee informs the Supervisor or Manager explaining the change needing to be made. Supervisor or Manager will verify that the changes should be made and will make sure that the documentation is updated via the IT department. The Supervisor or Manager will then ensure that the updated document is returned to the documentation folder and the older document is then disposed of.

DISPOSAL OF DOCUMENTS

Unclassified documents may be disposed of in the normal recyclable waste but classified documents must be disposed of either by placing them into a locked secure waste disposal or by shredding, whichever method is supplied to the department by CCS.

Unless required on a daily basis and used as instant reference all classified documents should be disposed of as soon as possible.

REFERENCE DOCUMENTS:

Occasionally it is easier to refer to a printed document than to keep referring to a stored folder or online document. If this is the case with a classified document, which should

normally only be a classification 1 document, then the Supervisor or Manager's permission must be sought and the document securely locked up when not in use.

Master Document List:

ID	Title	Issue Date/Version No:	Location	Authorised By