MCS CONTROL SYSTEMS LIMITED
Security Measures and Risk Management Policy

This policy is part of our Code of Ethics and is to be read in conjunction with our Social & Ethical Policy for Corporate Responsibility, Data Privacy & Protection Policy, Competition Law Compliance, Sustainable Development, Avoidance of Counterfeit Materials, Carbon Emission Reduction and Safeguarding policies, along with our commitment to SA 8000 Social Accountability and the Global Compact.

This policy is practised throughout our organisation from recruitment, through selection, training, promotion, discipline and dismissal.

At no stage in the past has the company or any of its Directors or employees been guilty of any social or ethical infringements.

GENERAL

This is to read in conjunction with SF260P – ISO27001 – Information Security Policy, SF279 - MCS Data Privacy & Protection Policy, SF242 Disaster Recovery / Business Continuity policy and SF197 - Business Risk Register.

This security policy includes Personnel & Infrastructure, Information Security, Electronic Security (Cyberthreat, Computer Virus, Electronic Communications & VPN), Procedures and External Threats.

This policy contains sections that, without formal reference, would be describes as our "User Management Access Policy".

All users are required to understand this policy and accept personal responsibility for adhering to its requirements.

As per all policies, this is renewed annually, as reflected by an expiry date, when the policy is reviewed at board level and re-issued.

All risks to our enterprise are covered within our formally approved Disaster Recovery / Business Continuity policy and Business Risk Register, which include all measures to be taken in the event of any unforeseen circumstances that could affect the business. This is reviewed on an annual basis as part of our insurance renewal.

The Managing Director has ultimate responsibility for this policy, however he has delegated responsibility to our internal IT Manager, who has the empowerment to carry out the necessary policy and procedural changes and management to maintain our systems through our outsourced IT provider.

MCS has carried out a full risk assessment (SF133IDS) to consider all security issues, which are reflected within this document.

Any breach of this policy by users will be regarded as misconduct, and will be subject to the company's disciplinary policy.

REGULATIONS

MCS is fully conversant with the requirements of ISO/IEC 27001, which specifies a management system that is intended to bring information security under explicit management control. To this end we have implemented the following controls.

MCS complies with the Immigration, Asylum and Nationality Act 2006, with the Centre for Protection of National Infrastructure (CPNI), Baseline Personnel Security Standard (BPSS), BS 7858:2006 and GDPR (General Data Protection Regulations).

CPNI, Centre for Protection of National Infrastructure, provides integrated (combining information, personnel and physical) security advice to protect national security, by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

Whilst MCS does not have an existing relationship/association with the CPNI, we are aware of their requirements and services and all of our policies have been developed around these requirements.

A Baseline Personnel Security Standard (BPSS) (formerly Basic Check (BC) will evidence current criminal record and unspent convictions under the Rehabilitation of Offenders Act 1974. A BPSS provides a level of assurance to the trustworthiness and integrity of individuals whose work involves access to confidential assets or information. There are no access restrictions for this level of disclosure and the result may be sent to the applicant or the employer.

Department for the Environment Food and Rural Affairs (DEFRA) has lead responsibility for the Water sector.

PERSONNEL

Recruitment of Employees & Sub-contractors

- MCS is constantly striving to keep abreast with the latest technologies & techniques and to this end we regularly review workforce requirements, with a view to recruiting the most experienced employees.
- When recruiting staff or contractors, we always check identities, with original passports vetted and copies retained. References are required and followed up, in all cases, to ensure that any potential employee does not and will not pose a threat, or may be targeted by terrorists.
- We are satisfied that all of our employees do not and will not pose a threat, or may be targeted by terrorists. We have written statements to back up this knowledge. MCS comply with the Immigration, Asylum and Nationality Act 2006, with the CPNI, the Centre for Protection of National Infrastructure and BS 7858:2006.
- All direct and indirect labour to be employed is recruited through recognised recruitment agency professionals. The use of these professionals assures us that the recruitment process has security checks built in.
- Recruitment processes are based on BS 7858:2006 - Security screening of individuals employed in a security environment.
- The code of practice gives recommendations for security screening of individuals to be employed in an environment where the security & safety of people, goods or property is a requirement of the operations where, security screening is in the public interest.
- All applicants are required to supply a CV in advance of an interview and complete an application form.
- References are required from all applicants and followed up in all cases.
- Employment will not commence until screening has been carried out (by telephone if necessary).
- Where an individuals are to be offered employment, they will be asked to assist in providing the following:
  - Confirmation of identity – Valid full passport, original birth & marriage certificate (where relevant), or military service documents.
  - Confirmation of the proof of right to work in the country where employment is being sought.
  - Confirmation of professional qualifications.
  - Confirmation of references - Should be established by direct reference to former employers, government departments, educational authorities, etc., with confirmation in writing and a continuous record of employment or history for 10 years, or back to school leaving, whichever is the shorter.
    A minimum of 2 references must be taken up; one of which (if applicable) is to be from the individual's most recent employer. If joining straight from school / college / university, we will request references from the relevant establishment.
    All references should be independently validated with the originator to ensure authenticity.
  - Declaration for reviewing of impairment convictions - Applicant is required to declare details of all cautions and / or convictions for criminal offences, including motoring offences and pending action not covered by the Rehabilitation of Offenders Act 1974.
  - Confirmation of good character - the company will obtain two written character references from two relevant persons with personal knowledge of the person being screened (one should be the most recent employer wherever possible).
  - Confirmation of no conflict of interest – from a business and / or personal perspective
- We have a statement from our recruitment agency to back up this requirement.

Employees

- Upon commencement of employment all new, redeployed and sub-contract / agency personnel are provided with comprehensive Inductions, giving clear instructions on our policies for all of their required areas of work, which include reference to our employee handbook, in which we outline the security measures to be implemented on a day to day basis.
- Security awareness is part of our culture and we ensure security is represented at a senior level.
- We ensure that employees understand and accept the need for security measures.
- All employees are issued with key fobs for clocking in & out purposes.
- Regular training sessions are Company Policy. Training is provided in-house for a variety of Health & Safety issues and all employees carry CSCS, SHEA & Water Hygiene cards. We will be running full training sessions based upon our security policy.
- Internal monitoring of the labour is carried out using our quality procedures. (Copy available on request).

Sub-Contractors / Third Parties

- MCS operates a strict policy that no subcontractors or other third parties are allowed access to any of our systems.
- All sub-contractors work on our systems without the ability to utilise removable media. This maintains the control of access as well as reducing the potential for any breaches to security.
- Subcontractors to whom we supply equipment are set up as users on our system and their access is controlled as any normal user, i.e. via the MCS manager responsible for them. When they leave MCS employment their account is disabled as any normal user.
- Subcontractors who supply their own equipment are not connected to our network and are not given authorisation to our systems. Data is transferred to/from them via removable media or e-mail and is controlled by the MCS manager responsible for them.
- We are not aware that we are associated with any high-profile individuals that might be terrorist targets.

Visitors

- All visitors have to report to reception, where they sign in and are issued with passes, which are returned upon their departure.
- Visitors are accompanied at all times.

Supply Chains

- All suppliers are approved prior to any orders being placed. This is in accordance with QA procedures.

INFRASTRUCTURE

Buildings, Contents and Equipment

- We are satisfied that our buildings do not pose a threat, or might attract terrorist attacks, however we do carry out works for nuclear establishments and water authorities, which may be targeted.
- All building are locked when unoccupied and protected by dual-protection intruder alarm systems, which are linked to the security services by both a hard wired system and mobile system, via the GSM network, to ensure that the alert is sent to the control centre.
- All risks to our enterprise are covered within our SF242 Disaster Recovery / Business Continuity policy, which includes all measures to be taken in the event of any unforeseen circumstances that could affect the business.
- We ensure good basic housekeeping throughout our premises.
- Public areas are kept tidy and well-lit, with any unnecessary furniture etc removed and garden areas kept clear.
- We have the minimum of access points to our buildings.
- Parking is controlled and where possible we do not allow unauthorised vehicles close to our buildings.
- MCS have installed appropriate physical measures such as combination locks on all doors, including the server room, one way (exit) security break glass locks on fire escapes, CCTV systems, complementary lighting outside buildings & glazing protection as required.

Installations and/or Services Vital to the Continuation of the Business.

- This is not considered to be a threat to our business.

INFORMATION SECURITY

Electronic Information

- We have considered the best ways to protect our information and take responsible IT security precautions.
- MCS have produced disaster recovery / business continuity plans, to ensure that we can continue to function without access to our main premises and IT systems.
- We currently have a structure whereby an existing user's access rights are approved by the user's Line Manager.
  If required, the Line Manager will seek written approval from a Director.
  The same applies for requests for additional access. All access is ultimately controlled by our formally approved IT supplier.
- The above also applies for changes in job role.
- All directories on our server are subject to strict controls with authorised access granted by Directors and initiated by the IT Manager.
- For new users, form SF214 details the required access and is completed by a Director or Senior Manager prior to the user starting.
- Internally, all PC's are password protected using RSA MD-4 standard encryption, with only the dedicated user knowing the password.
  Owing to the size of MCS, it would be unjustified to have separate servers for each customer or separate project.
  All passwords are required to a prescribed format to ensure compliance with these guidelines and must include at least one of each of the following – Upper case letter, Lower case letter, number and at least 8 characters long.
  Our system has default built in control ensuring password protection is renewed every 40 days, or within 9 days of the renewal date.
  PC screens must lock automatically after a period of inactivity and be password protected.
- MCS operates a strict policy that no third party is allowed access to any infrastructure or systems, as all access rights are controlled through our external service provider, as detailed below. Access is only allowed with provision of hardware managed by ourselves.
- We have considered the options for a business wide encryption policy on our systems however we believe the information that we have is not sensitive enough to warrant this on all devices. Security critical information will be provided on encrypted media.
- All information is backed up at a remote location.
- Upon leaving the company all access rights are removed immediately.

Back-Ups

All information is saved to the server, which is in a separate building to the back-up tapes.

We have a NAS box that creates a backup of all the data across all of the servers, which is then copied simultaneously to an external server, housed across several locations throughout the UK. This is managed and maintained by our external IT specialist, OGL Computer Services Group (ISO27001 accredited).

Weekly back-ups are put on to an external hard drive and removed off site once complete.

Back-ups are tested on a weekly basis.

To date, we have not encountered any failures.

Computer Virus Policy

Policy & Procedures

MCS Control Systems has adopted the following procedures for dealing with cyber threats and computer viruses:

1. As part of the IT induction programme, all potential users will be informed of their responsibility for security against malicious software and the practical steps they must take to keep this protection active and up to date.
2. All computers, desk top, lap top or otherwise and related computer hardware, attachments etc, owned by the company will be supplied with the latest appropriate anti-virus product and spyware with automatic updating.
3. Our operating systems are regularly updated by the IT Department. These updates provide software security patches that "patch up" holes in the system that may otherwise allow hackers access.
4. All employees are aware of the requirements relating to removable media.
5. E-mail attachments will be scanned by an anti-virus product.
6. All employees are aware of their responsibility to not open any e-mails that are from unknown sources. If accidentally opened, not to click on any links provided or post these messages on to any colleagues and friends, but to just delete them.
7. If suspected that a computer is infected with a virus, it must be reported to our external service provider, as below, or IT Manager.
8. All employees are reminded of the advice and instructions provided relating to the “Junk E-Mail” folder.
9. All personal computers connected to the company network must run an **approved** and **up-to-date** anti-virus product that continually monitors for malicious software (virus, worms, Trojans, etc).
10. No one is permitted to stop anti-virus definition updates and anti-virus scans except for domain administrators.
11. Any activity intended to create and/or distribute malicious programs onto the company network (e.g. viruses, worms, Trojans, etc.) is strictly prohibited.
12. The Company reserves the right to disconnect any machine from the network if an infection is found or suspected. The machine will be disconnected until the infection is removed.

Overview

Computer viruses pose considerable risk to the computer network. Viruses can cause the systems on the computer network to run erratically and lose or corrupt information. This could result in loss of productivity both at MCS or customers’ sites, loss of reputation with customers and loss of future business, or potential breaches of legislation.

This policy is an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It also defines what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the company’s network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the company from outside the company’s network be scanned for viruses by a specific program.

This policy is designed to protect the organisational resources against intrusion by viruses and other malware.

Scope & Objectives

It is our policy to ensure that:

- All staff are aware of their responsibilities in relation to safeguarding the confidentiality, integrity and availability of data and software within the company’s computer network;
- Best practice concerning the use of software is identified;
- The ways of preventing virus infections, and the steps that should be taken if a virus is found, are known.
- This policy applies to all authorised users of the company’s computer network.
- Access to the company’s computer network is only possible using computers issued by the company which are installed with company-approved anti-virus software.
- Users must not make changes to the configuration of our anti-virus software or install any other anti-virus software products.

Responsibilities

All users of the company’s computer network are responsible for their own adherence to this policy.

The company must comply with the GDPR (General Data Protection Regulations). This policy must be adhered to and is one of the ways the company can protect its personal identifiable data from loss, damage or destruction.

Protecting the Business from a Computer Virus

Permanently connected broadband internet is normal practice and it is increasingly easy for viruses to spread between machines.

These days every business has at least one computer that contains vital information. The protection of that information is essential.

Computer viruses continue to become more elaborate and the right precautions are needed to prevent the infection of business computers, to avoid losing client information or protected business practices to a hacker.

Up To Date Operating System

Virus writers exploit mistakes or bugs in the operating system, in order to install viruses or help them spread.

Once these problems are known, Microsoft issues fixes to prevent this.

Both MCS and our external service provider, as detailed below, utilise systems to ensure that our operating systems are regularly updated to remove the threat of these viruses.

Up To Date Web Browser

Ensuring that you are using the latest version of your web browser will help keep you secure.

Virus writers love bugs (mistakes in the software) in your web browser, they can use them to smuggle viruses aboard your PC. Once the web browser provider companies find out about these mistakes, they issue software updates to correct them.

Anti-Virus Software Controls

Anti-Virus software must only be installed and configured by the IT department.

Users must not disable or interfere with the anti-virus software installed on any PC.

No computer may be connected to the network without up-to-date anti-virus software being installed and activated by the IT department.

Only laptops owned by the company may be connected to the network, unless prior permission has been obtained from the IT department to connect a non-company laptop.

Users who operate their laptops on and off the network must regularly connect to the network to ensure that the anti-virus software virus definitions remain up-to-date. Failure to do so could result in unnecessary virus outbreaks.

User must not connect company laptops to non-company networks, unless they have obtained authorisation from the IT department.

No software programs or executable files shall be downloaded and installed onto a PC without permission from the IT department.

Unauthorised downloading of software may breach the copyright licence, could introduce a computer virus or other malware to the company's computer system, and is a breach of the company's Internet policy.

Any software provided by the company must not be installed onto equipment not owned by the Company.

All software installed on company PCs must be properly licensed.

The unauthorised copying of software is a criminal offence under the Copyright, Design and Patents Act 1988.

Avoiding Virus Infection

To avoid computers becoming infected by computer viruses, users must:

- Manually scan removable media for viruses. If needed, users should seek advice from the IT department on how to do this.
- Not switch on a PC with removable media in the respective drive, unless instructed by the IT department.
- Use network file storage facilities wherever possible (shared drive, home drive) to store computer files. Files in these areas are backed-up. If a virus infection does occur and the anti-virus software cannot repair any ensuing damage, it may be possible to restore files to a clean state from the backup media. (This is not possible for files stored on the C: drive or a removable medium.)
- All email attachments are automatically checked for viruses before they leave or enter the company's email system.

Users who have any suspicions regarding the integrity of any software should contact the information service desk.

Dealing with computer viruses

There are many viruses on the internet, but with a few simple precautions it is easy to stay safe from this online threat.

Utilising good Antivirus software is only part of the solution and we detail further good practice procedures below:

What are Viruses, Spyware & Trojans?

A virus is a piece of self-replicating code, most often a malicious software program ('malicious software'), designed to destroy or damage information on computers or steal user data. Computer viruses are computer programs, just like all other software that runs on your PC. What makes computer viruses different is that they are designed to copy themselves, throughout your computer's memory or hard drive, or even across the internet.

Many computer viruses have malicious components too, and may try to cause all sorts of problems from slowing down your computer to allowing hackers to gain entry.

There are many potential sources of malicious software, including websites, shared media, electronic mail and software or documents copied over networks such as the campus network or the internet.

Malware or malicious software is designed to infiltrate or damage a computer system without the owner's informed consent.

An infection by malware can be very costly. This may be through the loss of data, staff time to recover a system, or the delay of important work. Additionally, malicious software can spread from an infected system and can lead to reputation damage.

Malware is derived from the words "malicious" and "software". The expression is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software or program code.

Malicious software is a constantly evolving threat and MCS must therefore apply controls to protect our systems and information from all forms of malicious software.

While some of these are able to erase information, they cannot erase backup CDs and they cannot cause computers to explode!

Spyware is software specifically designed to watch things you do on your PC, perhaps to gather data on the websites you visit, or music you listen to. Plain spyware does not copy itself or exhibit other malicious behaviour, although many computer viruses are also spyware or contain spyware components. Not all spyware is necessarily bad.

Trojan horses or Trojans install a malicious program (the 'Trojan') without the user's knowledge. Once installed on a PC, Trojans send personal information or other data from the PC to a location somewhere on the Internet where it is then exploited.

The term is derived from the classical myth of the Trojan horse. Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

Trojans may look like games, or pictures, or other files which may seem to be fun to play with. The problem is that when you click on the file you will get a nasty surprise as a computer virus or malicious program lurks inside.

Trojans can also allow individuals with malicious intent to take remote control of computers for their own purposes.

Therefore, users must not download or install software not authorised by the IT department - downloading or installing unauthorised software is the quickest way to spread Trojans.

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other PCs on the network and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

A computer virus is a computer program that can copy itself without permission or knowledge of the user.

A virus can only spread from one computer to another when its host is taken to the uninfected computer; for instance, by a user sending it over a network or carrying it on a removable medium.

A computer virus hoax is a false message warning the recipient of a virus that is going around.
They are normally received via email, often in the guise of a warning or plea; with a request that the recipient sends the message to everyone he or she knows. Such messages can take the form of official looking warnings of viruses, chain letters or any message that asks the recipient to forward the message on to many people.
Most hoaxes are easily identified by the fact that they say the virus will do impossible things, like blow up the recipient's computer. They often claim to be from reputable organisations such as Microsoft and IBM, but include emotive language and encouragement to forward the message which would not come from an official source.
Many spam e-mails are sent about viruses with dire warnings or messages with topical subjects or attachments.
Any e-mails that are from someone you don't know or don't recognise, are to be deleted because they likely contain a virus.
If you do accidentally open one of these e-mails, don't click on any links provided within the body of the e-mail, as they likely link to a fake website that will download a virus automatically.
The message usually serves as a chain email that tells the recipient to forward it to everyone they know.
Do not post these messages on to any colleagues and friends. If you receive such messages, just delete them.
If you want to check its validity, forward the message to our external service provider, as detailed below, or talk to the MCS IT Manager.

Removable Media

- Removable Media is any form of medium or device that can be connected or inserted into a PC that contains readable information, such as memory sticks, dongles, floppy disks, CDs, or DVDs.
- All employees are clearly instructed in policy requirements concerning removable media and provided with a copy of this document.
- Any removable media that have come from outside the company, or have been used on a non-company machine, must be manually virus scanned before it is accessed.

E-mail Server & Malware Scanning

In addition to having the standard anti-virus program, the e-mail server or proxy server will have additional protection against malware since e-mail with malware must be prevented from entering the network.
This additional protection will scan all e-mail for viruses and/or malware as they enter the server and before they leave.
The scanner may also scan all stored e-mail once a week for viruses or malware.
When a virus is found or malware is found, the policy shall be to delete the e-mail and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the e-mail and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

Threats from Email and the Internet

Email is one of the main ways used to distribute computer viruses. This is due to the ease with which information can be distributed globally. Viruses can be hidden in email attachments, or in material downloaded from the Internet.
To help prevent viruses, worms and other malware being distributed over the company's network, users must:

- Make sure they know the sender of the email is genuine before opening any attachments. If there are any suspicions, the sender should be contacted by phone to confirm he or she sent the email.
- Contact the information service desk if they believe an email containing a virus has been received, or if the anti-virus software on a PC has detected a virus.
- Not download or install any software that has not been approved by the information department, e.g., music, screen savers, games, etc. Such software may contain malware.
- Not act on any emails that suggest they have been sent to fix a problem with a PC (e.g., emails indicating that they are from Microsoft). Reputable vendors would never distribute fixes to computer programs in this way. (The exception to this would be authorised software clearly marked and sent by the information department.)
- Not open emails if any suspicions regarding the integrity of its content. The information service desk must be contacted immediately.
- Not use unauthorised, web-based email services (e.g., Hotmail, Yahoo! Mail, Gmail, etc.).

Care with Attachments

Just because an attachment came from somebody you know, doesn't mean it is safe.
Before opening an attachment, at least read the rest of the e-mail. It is usually easy to tell if an E-mail has been written by a virus rather than a human. Antivirus software can help you here by automatically detecting if an attachment is safe.

Junk E-mail

MCS has a method for dealing with spam, which learns from you which e-mails are spam and which are genuine.
Any e-mail that the system thinks is spam will be automatically placed in your "Junk E-Mail" folder, which should be periodically checked to ensure that it does not contain genuine e-mails.
Two public folders have been created called "This is legitimate e-mail" and "This is spam e-mail".
To view these folders in Outlook, click on the "Folder List" button (by default this is at the bottom left of the Outlook window), then navigate down through "All Public Folders" and "GFI AntiSpam Folders".
If your junk e-mail folder contains a legitimate e-mail then drag the e-mail to the "This is legitimate e-mail" folder. Any future e-mails from this user will now be treated as legitimate e-mail and not spam. To keep a copy of the e-mail you may want hold down the CTRL key while dragging - this will 'copy' rather than 'move' the e-mail.
If your inbox contains a spam e-mail then drag the e-mail to the "This is spam e-mail" or "Junk Email" folder. Any future e-mails from this user will now be treated as spam.

Electronic Communications

MCS respects the privacy of users of electronic communications, which include e-mail, internet & telephone, however users should be aware that these are monitored and interceptions may be made in certain circumstances under the terms of The Regulation of Investigatory Powers Act 2000.

It is recognised that employees can use electronic communications for personal means and this policy will not prevent employees from continuing with this. However the Company requests that the use of electronic communications is not abused and should never interfere, either by its timing or extent, with the performance of the employee's duties.

It is requested that such personal use is confined to non-working hours whenever possible.

Email

Email should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter, memo or fax is equally unacceptable in an email.

Employees are not to send messages that are in any sense inappropriate (obscene, defamatory or otherwise).

Employees should be careful that before they open any attachment, they are confident that the content is in no sense inappropriate. Equally, if an employee receives an inappropriate email, whether unwittingly or otherwise and from whatever source, they should not intentionally forward the email to any other address, except to the IT Manager for investigation reasons.

The use of email to send or forward messages or attachments which are in any way inappropriate will be treated as misconduct under the appropriate disciplinary procedure. In serious cases this could be regarded as gross misconduct and will lead to dismissal.

Where the Company has reasonable grounds to suspect misuse of email, it reserves the right to monitor the destination, source and content of email to and from a particular address (see also recording of telephone calls and monitoring use of telephone, email and internet below).

The Company also reserves the right to access an employee's email account in their unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide them with prior knowledge.

Use of the Internet

The primary reason for Internet access, is for the easy retrieval of information for research purposes, in order to enhance the ability of employees to undertake their role. However, as with email, it is legitimate for employees to make use of the Internet in its various forms for personal purposes, as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

It is recognised that there can be occasions where it is sensible for the employee to make occasional use of the Internet for personal reasons, such as a bank transaction or the booking of a holiday, rather than spending considerably more time out of the office.

Unauthorised Internet use is treated as misconduct and in serious cases could be treated as gross misconduct and lead to dismissal.

The Company reserves the right to monitor the use of the Internet from particular personal computers or accounts where it suspects misuse of the facility (see recording of telephone calls and monitoring use of telephone, email and internet below).

Recording of telephone calls and monitoring of use of telephone, email and the Internet

It is the Company's policy that no employee is permitted, as a matter of routine, to monitor a fellow employee's use of the Company's telephone or email service, or of the Internet via the Company's networks. (The only exception is where designated Officers are authorised to receive print-outs of telephone call details from particular extensions for recharging purposes).

However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Directors, or in exceptional circumstances, authorised delegated personnel, may grant permission for the recording of an employee's telephone calls and for the monitoring of use of telephones, email or the Internet.

Once approved, the monitoring process will be undertaken by designated employees acting, for operational purposes, under the direction of the Directors. These employees are required to observe the strictest confidentiality when undertaking these activities and they will record or monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Directors, who will determine the actions that may need to be taken in any particular case.

When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis, with a view to terminating monitoring in as short a time as possible.

Employees who suspect misuse should advise a Director in confidence.

Copyright & Patents

The Company does not accept any responsibility, should an employee be in breach of the Copyright, Designs and Patents Act 1988, where this occurs outside of the workplace.

Virtual Private Network (VPN) Policy

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.

This policy provides guidelines for VPN connections to the MCS network and applies to employees utilising VPN's for network access.

No unauthorised persons are permitted to access the MCS network. It is the responsibility of personnel with VPN privileges to ensure that unauthorised users are not allowed access to MCS internal networks.

The VPN user will also be subject to the conditions and performance constraints of their chosen Internet Service Provider (ISP).

Approved MCS employees may utilise the benefits of VPN's, which are a "user managed" service. This means that the user is responsible for selecting an ISP, coordinating installation, installing any required software and paying associated fees.

VPN use is controlled using password authentication.

VPN gateways will be set up and managed by MCS Control Systems IT Management team.

All computers and other equipment, such as USB devices, connected to MCS Control Systems internal networks, via VPN or any other technology, must use the most up-to-date anti-virus software.

VPN users will be automatically disconnected from the MCS network after sixty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

For security reasons, VPN users can be disconnected, at any time, based on the company's discretion. VPN access may also be removed, at the discretion of the business, where a VPN user has a period of sickness or unexplained absence.

Penetration Test and Vulnerability Assessment

Our external service provider, as detailed below carry out random Penetration Test & Vulnerability Assessments on our infrastructure and systems. These will be carried out at least annually.

These penetration tests will identify, assess and record any potential information security risks to our company.

Dedicated Professional IT Security Services

In order to ensure that our systems are protected to the highest level, MCS has engaged a leading provider of IT & telecommunications services to provide specialist IT support & maintenance services, networking and business security.

OGL Computer Services Group, also described as “The IT Department”, are a dedicated Microsoft Gold Certified IT services provider.

This out-sourced professional service ensures our critical infrastructure is provided with both on site and offsite security measures.

Their contact details are: OGL Computer Services Group Ltd, Worcester Road, Stourport on Severn, Worcestershire, DY13 9AT. Telephone: 01299 873873 - Technical Service Desk Email: techsupport@ogl.co.uk. - Software Support Desk Email softwaresupport@ogl.co.uk.

WebLock Firewalls

We utilise WebLock, which provides comprehensive protection against network, content and application-level threats. These include complex attacks favoured by cybercriminals, without degrading network availability and uptime. WebLock platforms incorporate sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain (VDOM) capabilities to separate various networks requiring different security policies.

These series provide a comprehensive and high-performance array of security and networking functions including:

- Firewall, VPN, and Traffic Shaping
- Intrusion Prevention System (IPS)
- Antivirus/Antispyware/Antimalware
- Web Filtering
- Anti spam
- Application Control (e.g. IM and P2P)
- VoIP Support (H.323. and SCCP)
- Layer 2/3 routing
- Multiple WAN interface options

Security services by technology

- WebLock combines the multiple security technologies needed to protect modern organisations in a scalable, integrated fashion.
- WebLock offers the industry's broadest suite of security technologies under a single, consistent management interface for easy deployment and management.

Antivirus

- WebLock antivirus technology combines advanced signature and heuristic detection engines to provide multilayered, real-time protection against both new and evolving malware attacks in all web, email, and file transfer traffic.

Antispam

- WebLock antispam technology offers a wealth of features to detect, tag, quarantine and block spam messages and malicious attachments.

Database Security

- WebLock database security technology provides centrally-managed, enterprise-scale, database hardening; fast, comprehensive policy compliance and vulnerability assessment for improved data security across the enterprise.

Firewall

- WebLock firewall technology combines ASIC-accelerated stateful inspection with an arsenal of integrated application security engines to quickly identify and block threats.

Intrusion Prevention System (IPS)

- WebLock intrusion prevention technology, available in all WebLock® and WebLockWifi™ platforms, can be installed at the network edge or within the network core to protect critical business applications from both external and internal attacks.

Virtual Private Network (VPN) - IPSec and SSL

- WebLock IPSec and SSL VPN technologies in Weblock platforms is tightly integrated with other security features such as firewall, antivirus, web filtering, and intrusion prevention, providing more comprehensive protection than VPN-only security appliances.

Web Filtering

- WebLock Web filtering technology, integrated into all WebLock appliances, blocks access to harmful, inappropriate, and dangerous websites which may contain phishing / pharming attacks, malware such as spyware, or objectionable content that can expose organisations to civil or criminal liability.

Wireless LAN (WLAN)

- WebLock wireless technology adds a critical layer of protection to wireless LANs by integrating security services such as antivirus, intrusion prevention (IPS), web filtering, antispam and traffic shaping to deliver multi-layered wireless security.

Web Application Security

- WebLock’s web application security solutions provide specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS providers. The WebLockWeb family of web application firewalls delivers integrated web application and XML firewalls to protect your web-based applications and internet-facing data.

PAPER DOCUMENTATION AND SENSITIVE INFORMATION

- All confidential information and documents, that are not required or waste, are shredded.
- For dormant accounts, when an employee leaves the company it is the responsibility of the internally appointed IT Manger to remove all access rights the employee had as well as archiving the information to a managed location.

PROCESSES & CRITICAL PROCEDURES

General

- All processes are carried out in accordance with ISO9001 Quality Assurance Procedures, which ensures traceability throughout all of our activities.
- We are not aware that our processes are associated with any high-profile organisations that might be terrorist targets.
- None of our processes are considered to be high profile, however we do carry out work for nuclear establishments & water sites, which may targeted by terrorists.

On-Site

- It is normal practice for site inductions to be provided by the main contractor or client, but when it is a requirement for MCS to carry out the induction form SF138 is utilised. A copy of this form is available upon request
- Prior to commencing work, sites are inspected by the MCS Health and Safety Manager and or the Site Manager / Supervisor. All aspects of site safety are covered, including the accuracy and effectiveness of the risk assessments, adequate control, PPE etc.
- The Site Manager is given the opportunity to raise any issues concerning them, request information, support, etc. and asked if they consider their level of training & knowledge to be sufficient for them to conduct their operations with confidence and safety.
- For specific activities, relevant & suitably experienced staff create risk assessments & method statements for work to be undertaken.
- The site supervisor carries out regular site inspections to ensure that all requirements are fully complied with. The Contract Manager will visit the site on a regular basis, either independently or with accompaniment of the H&S Manager. The Group Health & Safety Manager will make regular unannounced visits to site and carry out audits.
- Any points raised at site visits and audits are communicated to the relevant Manager or Director for action. Subsequent visits are used to ensure outstanding issues are closed out.
- Toolbox talks are delivered at site to personnel to cover issues raised during an inspection. These are carried out in accordance with the HSE and CITB guidelines.
- Site management arrangements, daily co-ordination meetings and lines of communications are to be established.
- Where work takes place in the vicinity of other contractors activities, protective measures must be clearly identified in method statements and strictly adhered to.
- MCS will always work closely with the client and other contractors on site to ensure that the project is carried out with the absolute minimum of risk to our own employees and those of other companies.

EXTERNAL THREATS

Theft of Information at disposal

Paper Waste

All confidential information and documents, that are not required or waste, are shredded and removed from site by an industry recognised and accredited disposal company.

Certificates of destruction are provided to follow relevant legislation and to provide us with a record of removal and destruction.

Electronic Waste

All electronic equipment, which holds sensitive or confidential information, that are not required or waste, are completely ‘flattened by our IT department and then removed from site by an industry recognised and accredited WEEE disposal company.

Mail, Deliveries & Suspicious Items

Instructions include the following:

- Do not touch suspicious items.
- Move away to a safe distance.
- Prevent others from approaching.
- Communicate safely to staff, visitors and the public.
- Use mobile phones away from the immediate vicinity of a suspect item & stay out of sight and behind hard cover.
- Notify the police.
- Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.

Neighbours

- We are not aware of any high risk neighbours that could be attacked and cause us to suffer any collateral damage.

Terrorist Actions

The following should be considered as part of a Security Plan:

- Instructions on how to respond to a threat (e.g. telephone bomb threat).
- A procedure for employees to raise concerns or report observations.
- Evacuation plans, including details on securing premises in the event of a full evacuation and when to re-occupy premises.
- Details for Liaison with the police, other emergency services and local authorities.
- A search plan.
- A communications and media strategy, which also includes handling enquiries from concerned family and friends.

GENERAL INFORMATION

Government and Media

We ensure that we are aware of the latest news from newspaper reports, news bulletins and the Chamber of Commerce, regarding the current security climate and recent terrorist activities.

Communication, Compliance & Reporting

This policy is practised throughout our organisation from recruitment, through selection, training, promotion, discipline and dismissal.
MCS has communicated this Security Measures and Risk Management policy and all other policies referenced within this document to all employees and it is a requirement for them to be complied with at all times.
It is expected of all employees, if they discover a security incident or a breach/violation or suspected breach/violation of these policies or procedures, to report it to the Directors as soon as possible. If required, this will anonymous and in complete confidence and the employee will not suffer any consequences.

Breaches/Violations in Policy or Procedures

Any security incidents or breaches / violations to this policy or our procedures will be investigated.
When security incidents or breaches/violations are detected, it is essential that they are resolved, without delay, with recovery actions operated and prevention procedures implemented for the future.
Any deliberate breaches or violations will result in disciplinary action and possible dismissal of any individuals.
MCS reserves the right to contact the necessary authorities if there are any breaches / violations to this policy.

Publicly available Information about the company

MCS has a website and the annual accounts are published, but no information considered as sensitive is publicly available.
This policy will be kept up to date, the policy and the way in which it has operated, will be reviewed every year.

Signed: SPoole **Name:** Stephen Poole **Position:** Group Managing Director

This Policy Statement will only be signed on the original copy (available upon request)

Date Issued: 02/01/19 **Review Date:** 02/01/20