Information Security Policy

1. Purpose

The purpose of this Policy is to safeguard information belonging to MCS Ltd. (MCS) and its stakeholder (third parties, partners, sub-contractors, clients or customers).

This Policy informs MCS's staff and other individuals entitled to use MCS facilities, of the principles governing the holding, use and disposal of information.

It is the goal of MCS that:

- Information will be protected against unauthorised access or misuse.
- Confidentiality and integrity of information will be secured.
- Availability of information / information systems is maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Physical and logical security will be maintained.
- Infringement of this Policy may result in disciplinary action or criminal prosecution.
- When information is no longer of use, it is disposed of in a suitable manner.
- All information security incidents will be reported to the Managing Director and investigated through the appropriate management channel.

Information relates to:

- Electronic information systems (software, computers, and peripherals) owned by MCS whether deployed or accessed at its office.
- MCS's computer network used either directly or indirectly.
- Hardware, software and data owned by MCS.
- Paper-based materials.

2. The Policy

MCS requires all users to exercise a duty of care in relation to the operation and use of its information systems.

2.1 Authorised users of information systems

Except for information published for public consumption, all users of MCS information systems must be formally authorised by appointment as a member of staff, or by other process specifically authorised by the Managing Director. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person. The "Network password policy" describes these principles in greater detail.

Authorised users will pay due care and attention to protect MCS information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- permission of the information owner
- the risks associated with loss or falling into the wrong hands
- how the information will be secured during transport and at its destination.

2.2 Acceptable use of information systems

Use of MCS's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people. The detail of acceptable use in specific areas may be found in the Appendix.

2.3 Information System Owners

MCS personnel who are responsible for information systems are required to ensure that:

1. Systems are adequately protected from unauthorised access.
2. Systems are secured against theft and damage to a level that is cost-effective.
3. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
4. Electronic data can be recovered in the event of loss of the primary source.
5. Data is maintained with a high degree of accuracy.
6. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
7. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and freedom of information acts.
8. Any third parties entrusted with MCS data understand their responsibilities with respect to maintaining its security.

2.4 **Personal Information**

Authorised users of information systems are not given rights of privacy in relation to their use of MCS information systems. Duly authorised personnel of MCS may access or monitor personal data contained in any MCS information system (mailboxes, web access logs, file-store etc).

2.5 Individuals in breach of this policy are subject to disciplinary procedures at the instigation of the Managing Director, including referral to the Police where appropriate.

MCS will take legal action to ensure that its information systems are not used by unauthorised persons.

3. Ownership

3.1 The Managing Director has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

A. Appendix: Subsidiary Policies

The detail of acceptable use in specific areas may be found in the following list of subsidiary polices:

1. Acceptable use policy

This **Acceptable Usage Policy** covers the security and use of all MCS information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all MCS employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to MCS business activities worldwide, and to all information handled by MCS relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by MCS or on its behalf.

Computer Access Control – Individual's Responsibility
Access to the MCS IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the MCS IT systems.

Individuals must not:
• Allow anyone else to use their user ID/token and password on any MCS IT system.
• Leave their user accounts logged in at an unattended and unlocked computer.
• Use someone else's user ID and password to access MCS IT systems.
• Leave their password unprotected (for example writing it down).
• Perform any unauthorised changes to MCS IT systems or information.
• Attempt to access data that they are not authorised to use or access.
• Exceed the limits of their authorisation or specific business need to interrogate the system or data.
• Connect any non-MCS authorised device to the MCS network or IT systems.
• Store MCS data on any non-authorised MCS equipment.
• Give or transfer MCS data or software to any person or organisation outside MCS without the authority of MCS management.

Internet and email Conditions of Use
Use of MCS internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to MCS in any way, not in breach of any term and condition of employment and does not place the individual or MCS in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:
• Use the internet or email for the purposes of harassment or abuse.
• Use profanity, obscenities, or derogatory remarks in communications.
• Access, download, send or receive any data (including images), which MCS considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
• Use the internet or email to make personal gains or conduct a personal business.
• Use the internet or email to gamble.
• Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
• Place any information on the Internet that relates to MCS, alter any information about it, or express any opinion about MCS, unless they are specifically authorised to do this.
• Send unprotected sensitive or confidential information externally.
• Forward MCS mail to personal (non-MCS) email accounts (for example, a personal Hotmail account).
• Make official commitments through the internet or email on behalf of MCS unless authorised to do so.
• Download copyrighted material such as music media (MP3) files and video files (not an exhaustive list) without appropriate approval.
• In any way infringe any copyright, trademarks or other intellectual property.
• Connect MCS devices to the internet using non-standard connections.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

While exercising technical support duties, it is acceptable for MCS personnel to use Mobile devices such as memory sticks, CDs, DVDs and removable hard drives. MCS personnel must use due care when transferring sensitive or confidential data (MCS, client related) and ensure that such data is securely wiped from devices after usage.

Software

Employees must use only software that is authorised by MCS on MCS computers. Authorised software must be used in accordance with the software supplier's licensing agreements.

Individuals must not:

- Store personal files such as music, video, photographs or games on MCS IT equipment.

Viruses

MCS has implemented centralised, automated virus detection and virus software updates within the MCS environment. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than using approved MCS anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of MCS voice equipment is intended for business use. Individuals must not use MCS voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use MCS voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls International operators, unless it is for business use.

Actions upon Termination of Contract

All MCS equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to MCS at termination of contract.

All MCS data or intellectual property developed or gained during the period of employment remains the property of MCS and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on MCS computers is the property of MCS and there is no official provision for individual data privacy, however wherever possible MCS will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. MCS has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

It is the responsibility of all MCS personnel to report suspected breaches of security policy without delay to line management

All breaches of information security policies are to be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with MCS disciplinary procedures.