ACCEPTABLE COMPUTER USE POLICY

Policy Statement: Information security policies are the principles that direct managerial decision making and facilitate secure business operations. They allow the organisation to manage the security of information assets and maintain accountability. This Policy covers protocols and procedures for use of the company's IT equipment, specifically its servers, networks, and broadband connections. It also includes devices issued by the company including laptops, tablets, phones etc. as well as any equipment owned by staff or third parties which the company permits to be connected to its network. This policy should be read in conjunction with the IT Policy and Data Protection Policy. This policy gives the organisation a structured framework to properly manage IT resources and data security.

All Employees: This policy applies to all persons working for or on our behalf of the McSence Group of Companies which includes the subsidiary companies - *McSence Communication Ltd, McSence Ltd, McSence Services Ltd & McSence Workspace Ltd* in any capacity including but not limited to:

- Directors, all employees at all levels, prospective employees, agency workers, seconded workers, temporary workers, contractors/sub-contractors, suppliers, clients, agents, external consultants, volunteers, members of the public, group's supply chain, third-party representatives and/or business partners who will be referred to in our Group policies as "all employees".

The Workplace: This policy applies to all persons working for or on our behalf of the McSence Group of Companies in any capacity at the workplace(s) as defined below which includes but not limited to:

- McSence Premises, Offices, Units, Business Park, Client's Premises, External Meeting Places, Customers' Homes, Gardens, Sheltered Housing, Whilst On-Call, On-Duty, Emergency Cover, Working from Home including On-Line Meetings, Whilst Driving in Company Time, Working Public Areas (café's, trains, coffee shops, buses etc) and will be referred to throughout this policy as "the workplace".

Purpose: McSence must ensure our IT systems operate efficiently, securely, and safely to protect our data and that of our clients, comply with GDPR and remain protected from cyber attacks or other digital threats. We must also ensure our assets are not used inappropriately, immorally, unethically or illegally. Employees have an obligation as far as reasonably practical to assist in this objective.

Roles & Responsibilities: Employees: Employees are required to follow the procedures set down in this Policy and to operate in a way which protects the best interests of the Company. In particular:

- Employees must be aware of acceptable computer use issues contained within the policy, the IT Policy and the Data Protection Policy and refrain from carrying out any activities likely to be a breach of this policy or recognised good practice while using company facilities and/or equipment as far as reasonably practical.
- Employees who have consent to use their own devices on the McSence system must do so fully in accordance with this policy as if it were a McSence issued device they were using.
- Employees must not use their own devices on the "staff" network and these should be restricted to the "guest" network only.
- Employees must not use McSence devices, network or broadband to conduct illegal activities or violate the law in any way.
- Employees must not use McSence devices, network or broadband for immoral or unethical purposes or in any way that would damage the organisation or bring it into disrepute or cause ill-will towards us.
- Employees must not attempt to:
    - Break the security of any computer network or user
    - Send junk email or spam
    - Send or receive a massive amount of email or data
    - Circumvent any company IT security measures such as bypassing or disconnecting the Fortinet firewall, turning off anti-virus software or amending security configurations without consent.
- Employees must ensure the security of all company issued equipment and report anything lost or stolen immediately they become aware.

- Employees must report any breaches or incidents likely to lead to a breach in this policy to their Business Unit Manager or the Chief Executive as soon as they become aware. Such instances would include suspected malware or virus attacks on either McSence or personal devices that have been connected to the network.
- Failure by an employee to follow the Acceptable Computer Use Policy as set out within this document will be considered a conduct issue and may be subject to action under the company's disciplinary procedure.
- A deliberate act of sabotage in the use of any Company IT systems or equipment or deliberately passing access information such as passwords to other parties with the intent of causing harm to the Company or its stake-holders will be regarded as gross misconduct and will be subject to action under the company's disciplinary procedure.

Business Unit Manager: The Business Unit Manager is responsible for supervising their staff in complying with the requirements of this Policy. In particular:

- The Business Unit Manager will monitor all employees under their control who are accessing Company IT systems and ensure adherence to this Policy.
- The Business Unit Manager will assess the IT competence of all new staff joining or being promoted or transferred into a new role maintain and maintain a record of this in their Training Matrix. This should identify any training needs for which the Business Unit Manager will be responsible for implementing.
- The Business Unit Manager will keep the Chief Executive informed of any recommendations for change or updating required to this Policy to support the Company's objectives.

Chief Executive: The Chief Executive has ultimate responsibility for this Policy and will act as the lead officer for all IT related issues. In particular:

- The Chief Executive will keep this policy under review and will update, as necessary.
- The Chief Executive will be responsible for appointing an experienced and competent IT Support Contractor and will review their performance from time to time.
- The Chief Executive will be responsible for maintaining suitable Cyber Protection Insurance assuming such insurance remains available in the marketplace at competitive rates.
- The Chief Executive may delegate some or all his responsibilities under this policy. All such delegations should be recorded in writing unless temporary due to absence in which case his duties will be undertaken by his nominated deputy.

Procedures:

General: McSence systems and information will be subject to monitoring at all times. Use of the McSence network and equipment constitutes acceptance of this monitoring policy. All McSence assets will be subject to inventory and inspection periodically for which staff must grant access as required.

Only licensed and approved software will be used on any Company devices. Only system Administrators may install software on Company devices. Employees are prohibited from downloading and/or installing software of any kind on company devices without the consent of the Chief Executive.

If staff require specific software in connection with their employment, they should refer this to their Business Unit Manager who should present a business case to the Chief Executive for approval. The IT Support Contractor will then roll out installation.

Unauthorised copying or distributing of copyrighted software is a violation of UK Copyright Law and will not be permitted.

Users must not allow non-employees to use any machine or device without authorisation from their Business Unit Manager or the Chief Executive.

Storage, development or the unauthorised use of tools that compromise security (such as password crackers or network sniffers) are strictly prohibited.

Sabotage, destruction, misuse or unauthorised repairs are prohibited on McSence devices or information systems.

Users must not carry out repairs or modifications to McSence devices or systems. If any such activities are required these must be referred to the IT Support Contractor by the Business Unit Manager.

Internet Use: Internet use represents the single largest risk to cybersecurity for the Company. Internet access is provided to enable employees to conduct Company business. While these resources are to be used primarily for business, the company realises that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

- Non-business Internet activity must be restricted to non-business hours or when staff are not working i.e., on a break.
- The definition of non-business use is the sole discretion of the Business Unit Manager. Such definition may change without notice as the Internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a McSence domain address (such as posting to newsgroups, use of chat facilities and participation in email lists) must not bring disrepute to the Company or associate McSence with controversial issues (i.e., sexually explicit materials).
- Internet use must not have a negative effect on the Company or its operations.
- Users will not make unauthorised purchases or business commitments through the Internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the Internet. Plagiarism or violation of copyright is prohibited.
- Release of McSence proprietary information to the Internet (i.e., posting information to a newsgroup or social media) is prohibited.
- All Internet users will immediately notify their Business Unit Manager of any suspicious activity.
- All remote access to the McSence internal network through the Internet will be encrypted and authenticated in a manner authorised by the Chief Executive and with his authority only.
- Accessing personal social networking accounts (including but not limited to Facebook®, WhatsApp®, Twitter®, Google+®, MySpace®, LinkedIn®, Foursquare® and TUMBLR®) or using McSence email for personal social networking purposes using McSence devices is prohibited. The use of social networking sites for specific business purposes must be pre-approved or assigned by a Business Unit Manager.
- Staff must not access web sites that display a “not secure” warning in the address bar and ***must not click on any hyperlinks*** unless they know these will lead to a secure site.

Email Use: Where necessary as a requirement of their post, employees will be provided with a company email address for business use. Employees should not use personal email accounts for business use, and it is prohibited to use a web based personal email account while connected to the McSence network. When using email, employees must abide by the following requirements.

- When sending email, users should verify all recipients to whom they are sending the message.
- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (ie, global send) is prohibited. This includes the forwarding of chain letters.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, colour, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (i.e., identification, addresses) is prohibited.
- Staff ***must not click on any hyperlinks*** contained within an email unless they are absolutely sure of their origin. In no circumstances should staff click on any links contained in an unsolicited email they may receive.
- Staff must not forward Company email information to their own personal email accounts or those of any other user unless there is a clear business need to do so and authority has been granted in advance by their Business Unit Manager.

All outgoing email will automatically include a footer statement which contains company identification and contact information and a limit on liability. This is a legal requirement, and the system should set this up automatically. It is

not permitted to delete or disable this and if employees become aware that for some reason it is not being automatically added to their outgoing emails, they should report this immediately to their Business Unit Manager.

All email communication is monitored. The Company uses an automated cloud backup service for its 365 system and any lost or misplaced emails can be retrieved by making a request through the IT Support Contractor. As such, staff should note that deleting an email message does not mean it has been deleted from the system.

Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.

Virus, Hostile and Malicious code: It is critical that the company and its assets are protected against attack from destructive or malicious programmes. To this effect:

- The IT Support Contractor will ensure that McSence obtains and deploys the latest in virus protection and detection tools and that this is maintained and updated automatically.
- All information systems media introduced to the McSence Ltd environment will be scanned for virus, hostile and malicious code.
- All emails will be scanned for virus, hostile and malicious code.
- All Internet file transfers will be scanned for virus, hostile and malicious code.
- Regular security scans will be carried out on all McSence systems and devices including data drives.
- Viruses that are detected will be quarantined or any other action required will be notified to users by the IT Support Contractor.

Some security updates and patched require devices to be re-booted before they become effective. If asked by Fortinet or Microsoft software to re-boot a machine, staff should do so as soon as it is convenient. As a minimum, all devices should be switched off when not in regular use or are unattended for a period of time and must be fully shut down overnight and restarted in the morning.

If staff think or suspect that updates are not being automatically carried out, they should report this to the IT Support Contractor or the Chief Executive immediately. Staff should check updates are regularly installed by visiting the "Update & Security" page within "Windows Settings" on their device.

Data Storage on the Company Server: Data files are stored on the server. The drive is organised into a number of folders relating to Business Units or activities with a number of Group folders for commonly used files. Access to these files is restricted to staff with the necessary privileges only. The IT Support Contractor maintains a schedule of users who are assigned to "Groups" with certain access permissions to certain data and any changes in access levels must be approved by the Chief Executive.

Staff must not change the architecture (layout or content) of the file structure without written consent from the Chief Executive and no security or access restrictions other than those already in place should be imposed without the express consent of the Chief Executive.

The data in these files is secure and there should be no need to individually password protect files but if the Business Unit Manager determines there is a business need for this, the password must be advised to at least one other member of staff so that data is not locked forever.

Staff may set up personal files within the area of the server they have access to, but any such information contained therein becomes the property of the Company for the purposes of this and all other IT policies and procedures.

Staff should not save files to the hard drive of their PC or laptop except in an emergency or as a temporary measure for a very short period of time as this is not backed up and cannot be controlled by the Company's data use or GDPR procedures.

Training: The Business Unit Manager will assess all staff joining and those changing job roles internally for competence in IT aspects of their role and record this on the Training Matrix for their department. Any training needs identified should be carried out as soon as possible in conjunction with the Training team. The company will provide training in

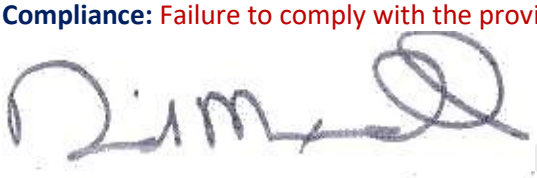
the application of this policy and also some general cyber-security training as part of the induction process for staff joining with an IT role to play.

Any staff who feel they need additional training in any aspects of this policy should raise this with their Department Manager either immediately they become aware or at their next regular performance review meeting.

Feedback: The Company are keen to engage with all stakeholders regarding policy or procedural matters at any time and all feedback regarding this policy including issues with compliance or areas where it could be improved would be most welcome. These should be directed to the Business Unit Manager or directly to the Chief Executive.

Company Intranet – Staff Zone: All the McSence Groups policies, procedures, handbooks are available on-line to all employees on the McSence Group's Staff Zone Intranet via our website Login | McSence

Compliance: Failure to comply with the provisions of this Policy may result in Disciplinary proceedings.



McSence Group Signatory:
David Maxwell | Chief Executive
McSence Group - *McSence Communication Ltd, McSence Ltd, McSence Services Ltd & McSence Workspace Ltd*
T: 0131 454 1500 | E: mail@mcsence.co.uk **| W:** www.mcsence.co.uk **| FB:** www.facebook.com/McSenceGroup

Policy Amendments & Revisions: *This policy will be reviewed annually and, if necessary, revised in the light of legislative or organisational changes Improvements will be made by learning from experience and the use of an established annual review. Should any amendments, revisions, or updates be made to this policy it is the responsibility of the Company Senior Management Team (SMT) to see that all relevant employees receive notice and training if necessary.*