P

OnSite Support Information Security Policy

This policy is not contractual and can be reviewed, amended or withdrawn at any time.

Table of Contents

Introduction

Information is an asset, which like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investment and business opportunities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access;

- **Integrity:** safeguarding the accuracy and completeness of information and processing methods;

- **Availability:** ensuring that authorised users have access to information and associated assets when required.

- **Traceability:** refers to the capability to keep relevant track and, when required, proof of what was done on our systems. Traceability also covers legal objectives such as nonrepudiation or accountability.

- **Compliance:** guarantees that our information systems operations comply with applicable rules, laws and policies.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organisation are met.

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image. Increasingly, organisations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking, and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means organisations are more vulnerable to security threats. The interconnecting of public/private networks and sharing of information increases the difficulty of achieving access control.

Appropriate management and procedures should support security that can be achieved through technical means. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organisation. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organisations may also be needed. It is essential that an organisation identifies its security requirements. There are three main sources of security requirements:

1. The assessment of risks to the organisation, taking into account the organisation's overall business strategy and objectives. Through risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated, and potential impact is estimated;

2. The legal, statutory, regulatory and contractual requirements that an organisation, its trading partners, contractors and service providers must satisfy, and their socio-cultural environment;

3. The set of principles, objectives and requirements for information handling, processing, storing, communicating and archiving that an organisation has developed to support its operations.

* Extracted from ISO 27002:2013 Code of Practice

Purpose:

To establish requirements for the protection of OnSite Support information technology services and the information assets they contain.

Scope:

This document describes the basic computer security measures that must be followed by all company employees authorized to use OnSite Support computer systems.
The policy objectives defined within this paper a based on those found within ISO 27001:2013 Information Security Management System.

Responsibilities:

Managers: All OnSite Support managers must ensure that their employees adhere to OnSite Support security requirements for the data and IT resources within their area of responsibility. Managers are also responsible to deny requests for unnecessary access to resources and to request removal of access to resources when they are no longer needed by employees.

Employees: OnSite Support employees must adhere to the security requirements established for the OnSite Support resources they own, manage, or use.

Third parties, Contractors and Service providers: These groups engaged by OnSite Support are to use, develop, deploy, and manage services in accordance with OnSite Support security requirements, and maintain auditable records demonstrating compliance with this instruction.

All procurement agreements with IT service providers must include descriptions of these responsibilities.

OnSite Support IT Security Policy

Clear Desk, Clear Screen

- OnSite Support IT services must only be used for conducting OnSite Support business or other purposes authorised by Senior Management.

- Information of a confidential nature should not be available for casual viewing or inspection by visitors to OnSite Support offices.

- All confidential information including client related documentation, personal identifiable information about OnSite Support employees or non-OnSite Support persons should be placed out of sight when a work area is unattended.

- Workstations should not be left unattended in a state where unauthorised Individuals could across applications or documents.

- OnSite Support staff should ensure that PC's or other devices are screen locked when left unattended; this can be achieved by using the CNTRL + ALT + DELETE or WINDOWS+L keys on desktop and laptop devices or by using the screen lock process in place for other tablet or smart phone devices.

- Do not leave your laptop unsecured overnight. Lock your laptop in a desk or take it with you.

Mobile Device, Bring Your Own Device (BYOD) and Remote Working
This section relates to the security of smart phones and tablets (e.g. Apple TM, Android, Microsoft TM devices etc) when working out of office premises.

At the discretion of OnSite Support, management will provide certain employees the option to use their personal owned devices e.g. smart phone or tablet for business

usage, including sending and receiving email, accessing OnSite Support and confidential information.

Staff who have agreed to use their personal owned devices for business must agree to allow to apply whatever security settings it sees fit to employ on the device, whether these be set using a mobile device management (MDM) tool or by any other means. If the employee does not want security settings to be applied to their personal owned device, they will be provided with an alternative provisioned device.

OnSite Support may supply mobile phones and other mobile devices e.g. smart phones or tablet to members of staff if required for the job role.

Employees who have been provided with an OnSite Support device or use their personal device for OnSite Support business must adhere to the following rules:
- All devices must have the screen lock functionality activated using a PIN or equivalent security setting on the device.
- Employees are responsible for ensuring the safekeeping of any telecommunication equipment used for OnSite Support business. Any theft or loss or fault of up owned or personally owned equipment must be reported to Helpdesk as soon as practically possible In order for the appropriate measures (e.g. data wipe) to be conducted.
- Use a carry case when transporting a laptop device. This will keep it dry, protect it from small knocks and keep it away from prying eyes.
- Do not leave devices in visible places e.g. a car or in a public place.
- When using the device to work remotely (e.q. on a train) ensure information on the device cannot be overlooked by non-OnSite Support personnel and keep the device secure, In such a manner as to restrict unauthorised access to the device.
- Ensure that any work carried out remotely is saved on OnSite Support systems or is transferred to OnSite Support systems as soon as is practically possible.

Passwords and Pass codes
It is a criminal offence under the Computer Misuse legislation to deliberately attempt to access or modify a system to which you have no authority. OnSite Support monitors systems; all unauthorised attempts at accessing systems will be investigated.

A unique username is the primary means of verifying your identity and subsequently enables access to OnSite Support systems and information. Passwords or pass codes that are used to gain access to systems or devices containing confidential information must be subject to the following rules:

- Must not be written down or kept where others might find them.
- Must not be shared with anyone; including administrators.
- Must be hard to guess and contain alpha numeric characters where appropriate.

Warehouse employees who do not have an OnSite Support employee ID, must request that their supervisor provide them with access to the necessary systems.

Malware (Virus)

Files obtained from sources outside the company, including portable media brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the company's computer network. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use data storage devices from non-company sources. Data storage devices must first be scanned and checked by the IT team using company-approved virus checking software. If you suspect that a virus has been introduced into the Company's network, notify the OnSite Support Service Desk immediately.

The purchase of all software for the Company must be formally authorised by the IT manager. All new software must be examined by the IT manager to ensure it is free from any virus and regular checks will be made for viruses. All software and disks must be purchased from recognisable reputable suppliers, backed by a confirmation that all such items are free from viruses etc. and/or with a guarantee/liability acceptance in the event that viruses which have caused damage are present on purchase.

Email and Internet Acceptable Usage

This code sets out the Company's policy with regard to use of e-mail and the internet:

Access to the e-mail and internet systems through the Company's networks and equipment are exclusively for the purpose of the Company's business and all e-mail messages and internet use are records which are the property of the Company. This code applies fully and equally to all Company laptops, Company computers installed in premises outside the Company's offices and other communication equipment. It also applies to all use of the e-mail and internet systems when accessed remotely through external systems.

The systems are not intended for private or personal communication or use. The Company reserves the right to forbid such use entirely.

All employees have a responsibility to use the Company's computer resources and the Internet in a professional, lawful and ethical manner.

You must not under any circumstances use the e-mail system or Internet to access, download, send, receive or view any materials that you have reason to suspect are illegal. Please refer to the second part of this Policy entitled "A Guide to the Legal Issues" for guidance on what materials may be illegal.

Please remember that it may be illegal to copy many materials appearing on the Internet including computer programs, music, text and video clips. If it is not clear that you have permission to copy materials off the Internet, please do not do so.

You must not send or circulate any materials on the Internet or by e-mail that contain any negative remarks about other persons or organisations. Any use of the e-mail system or Internet access for any of these prohibited purposes will be treated as a serious disciplinary matter which may lead to dismissal of the employee concerned.

Email Communication

Many Email communications you receive contain OnSite Support proprietary and confidential material, which should never be forwarded to people outside of OnSite Support.

As with all business records, Email is archived and can be retrieved and contribute towards legal proceedings, as permitted by local laws and jurisdiction. Like all communications, you should take care not to say anything that might appear inappropriate or be misconstrued by a reader.

The following rules must be followed when using e-mail:
- Care should be taken to ensure that data is sent or received virus free. Do not open or transmit any documents that you consider to be unsafe. All documents that are received from dubious or unsolicited senders should be forwarded to IT for checking.
- Never send any message, picture or joke, however well intentioned, which might cause distress to anyone or be seen as harassment. Remember that e-mails can have a much wider audience than was intended. The Company views any form of harassment or discrimination as a potential act of gross misconduct, which may result in dismissal. In cases which are seen as appropriate, we may also ask the Police to become involved.
- The system must not be used for the sending of adult/sexually explicit material.
- You should ensure that you do not make misleading, untrue or defamatory statements in any correspondence.

You must not respond to unsolicited e-mails of the 'junk' variety or participate in any 'chain letter' activity unless it has been specifically authorised by the Company. The vast majority

of these messages are bogus, some contain viruses and may slow down or damage our IT Systems.

All employees should be aware of the following:

Within the e-mail system the Company has installed content security software, which has the ability to filter incoming, outgoing and internal mall for viruses, non-business-related mail and attachments.

The Company has the right to intercept, monitor and review all e-mails, e-mail attachments, and internet use which are at any time on, within or accessed through the Company's systems, should they consider it necessary to do so for business purposes.

File sharing

The use of public cloud storage services not authorized by IT policy is prohibited. Examples include Dropbox, OneDrive, Amazon, 'Cloud etc, these all present security risks and are not suitable for the storage of company data.
For the secure transfer of data to third parties outside our network, please contact IT support for guidance to ensure data is encrypted and stored securely.
The use of personal USB sticks or drives is prohibited, if you need to transfer large files please contact IT Support who will be able to assist.

Spamming

This term is used to describe indiscriminate blitzing of e-mail messages to an entire community.

It is easy to e-mail everyone on the network but unnecessary traffic will soon clog the network and reduce the efficiency of e-mail (and other processes). Please think carefully before dispatching mass e-mails and only copy messages to those individuals who need to know.

Employees should avoid disclosing their e-mail address where it is likely that this will result in the employees receiving numerous e-mails which are not related to the business of the Company.

Social Media Use

'Social Media' or 'networking' sites refers, but is not limited to, the following online resources:

- Personal blogs
- LinkedIn
- Twitter
- Facebook
- Personal Web sites

- Community forums
- Internet chat rooms
- Online encyclopaedias - such as Wikipedia

Posting on social networking sites by employees, whether using the-property and systems or personal computer systems, is subject to the terms and restrictions set out in this policy. You are reminded that your duty of confidentiality to OnSite Support applies to social networking. As such, employees are prohibited from revealing any confidential or proprietary information, trade secrets.

Employees shall not engage, even in their own time, in any social networking; that may harm or tarnish the image, reputation and/or goodwill of OnSite Support and/or any of its employees, workers, suppliers or clients which is detrimental to onsite Support interests that involves bullying or harassment of, or making disparaging or derogatory comments about any of the employees, workers, suppliers or clients that involves posting or misusing other employees personal data or information, where that information has been accessed from the onsite Support without the consent of the other employee, OnSite Support reserves the right to routinely monitor all employees for the purpose of ensuring that OnSite Support rules are being complied with, investigating wrongful acts, or Complying with any legal obligation. You should have no expectation of privacy when using OnSite Support systems or property.

Any breach of this policy is likely to result in disciplinary action being taken. A serious, breach of this policy may be considered to amount to gross misconduct warranty-1 dismissal. The following are non-exhaustive examples of the type of behaviour that may be regarded as gross misconduct:

- Posting Company, client or supplier confidential information online
- Any form of harassment, bullying or discrimination against any of OnSite Support employees, workers, suppliers or clients
- Making derogatory, damaging or offensive comments or statements about any of OnSite Support employees, workers, suppliers, clients or competitors
- Online posting of personal data or information which you have obtained from'. about another employee or worker, without their consent
- Any activity that may bring OnSite Support into disrepute or damage or lower the company's reputation

Communication of Proprietary Information

You must not disclose any secrets or other information of a confidential nature relating to the Company or its business, or in respect of any obligation of confidence which the Company owes to any third party, during or after your employment except in the proper course of your employment or as required by law.

Any documents or tangible items which belong to the Company or which contain any confidential information must not be removed from the Company's premises at any time without proper authorisation and must be returned to the Company upon request and, in any event, upon the termination of your employment.

If requested by the Company, all confidential information, other documents and tangible items which contain or refer to any confidential information, and which are in your possession or under your control, must be deleted or destroyed.

Gross Misconduct

Any activities prohibited in this policy amount to misconduct and may result in disciplinary action, possibly including dismissal. (See the Disciplinary Policy for further information.)
The Company views the following as potentially amounting to gross misconduct:

- The unauthorised disclosure of personal passwords;
- The loading of unauthorised software;
- The downloading or sending of pornography, jokes, pictures, images or any other communication which may cause harassment or distress to the recipient;
- Any communication that discriminates against people on the basis of their gender, marital status, pregnancy or maternity, religion or belief, race, sexual orientation, disability or age;
- The deliberate or negligent introduction of viruses into the Company;
- The disclosure of confidential information to unauthorised sources
- The unauthorised duplication or distribution of copyrighted information;
- The failure to follow the rules contained in the 'Internet and e-mail Policy'
- Computer hacking;
- The sending of or circulating of defamatory information either internally or externally;
- The sending of unauthorised chain letters;

- Entering into unauthorised contracts online.
- Unauthorised access to confidential or private company information.
- Download/storage of data intended for personal use which does not contribute to the performance of your job.
- Unauthorised removal of company assets from premises.
- The use of company assets for day trading.
- The use of company assets for online auctions within office hours, unless pre-authorised for company business.

(The above list is not exhaustive)

As an employee of the Company, you also have the duty to inform **IT** if you receive any electronic communications that may amount to breaches of the Internet and e-mail Policy.

Security Incident Reporting

It is the responsibility of all employees to report security incidents. Security incidents should be reported to the IT Manager, your Line Manager or a member of the senior management team.
Incidents include:

- Physical security breaches of OnSite Support premises
- Loss of OnSite Support owned information
- Loss or theft of OnSite Support assets
- Malware (Virus)
- Misuse of systems
- Breaches of Laws
- System crashes

Employees are not to attempt to investigate or take action against the offender.

A Guide to the Legal Issues Relating to the Use of E-mail & the Internet

Introduction

This section of the Policy is intended to give employees guidance on the most important legal issues which may arise from their use of the e-mail system and Internet access.
It is very important that you read this section to understand those issues as this will help you, and OnSite Support avoid problems.

These are not just theoretical issues. If the law is broken, then this could lead to one or more of the following consequences:

- Civil and/or criminal liability for yourself and OnSite Support
- Disciplinary action against you including your dismissal.

Bullying and Harassment

OnSite Support requires all employees to be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be on the grounds of sex, race, disability, sexual orientation, age, religion. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by email. You must not send any messages containing such material.

Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal.

If you are subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation you are encouraged to contact your line manager immediately.

Breach of Copyright

Materials that you encounter on the Internet or receive by e-mail are likely to be protected by copyright. This will apply to written materials, software, music recordings, graphics and artwork and video clips. Only the owner of the copyright, or other persons who have the owner's consent, can copy those materials or distribute them.

If you copy, amend or distribute any such materials without the copyright owner's consent, then you may be sued for damages. OnSite Support may also be liable and, in some circumstances, criminal liability can arise for both you and OnSite Support.

Be particularly careful not to copy text or to download software or music unless you are sure you have permission to do so. Always check the materials in question to see if they contain any written prohibitions or permissions before you copy or download them.

Never download any software, music recordings or other materials that you know to be fakes or "pirate copies".

Failure to follow the Policy's rules will be treated as a serious disciplinary matter which could lead to dismissal.

Unwanted Contracts

An exchange of e-mail messages can lead to a contract being formed between yourself, or OnSite Support and with the intention that legal obligations should arise, and some payment or other consideration being made for the performance of those obligations. Breach of contract can expose OnSite Support to a claim for damages.

Contracting by e-mail is subject to the same requirements as any other form of contract. You must adhere to the established policies and procedures about purchasing and contracting.

Never commit OnSite Support to any obligations by e-mail without ensuring that you have the authority to do so. If you have any concerns that what you are doing will form a contract, contact the Managing Director.

Defamation

If you send an e-mail (NB: even an internal e-mail), or post any information on the Internet, which contains any remarks which may adversely affect the reputation of another organisation

or person, you will be exposing both yourself and OnSite Support the risk of legal action for defamation.
This is a real risk. Companies have been sued for the defamatory contents of e-mails sent by employees and have been required to pay out considerable sums as a result.

Obscene Materials

You must not under any circumstances use the e-mail system or Internet to access, display, circulate or transmit any material with a sexual content. This may constitute a criminal offence and both OnSite Support and you personally could be liable. Sexual harassment will be treated as a serious disciplinary matter which may lead to dismissal.

Protection of Personal Data & GDPR

Please note that OnSite Support is required to comply with legislation concerning the protection of personal data. Failure to adhere to that legislation could expose OnSite Support to civil liability, with The Regulator able to impose significant fines for non-compliance of up to 4% of annual worldwide turnover.
Obligations under GDPR legislation are complex but you can help ensure compliance by adhering to the following rules:

- You must get consent to hold data on a person, and you must explain why you hold that data and for how long.

- A person can ask you for information you hold on them and you are obliged to provide it. Information includes written and digital records.
- A person has the right to demand that you remove their details from your records.
- If you transfer data outside your geographical border it must be protected.

Data security

- The Company takes the security of HR-related Data seriously. [The Company has internal policies and controls in place to protect Data against loss, accidental destruction, misuse or disclosure, and to ensure that Data is not accessed, except by employees in the proper performance of their duties.]

- The Company maintains adequate technical and organisational security measures designed to safeguard the Data of employees against unauthorized access or disclosure.

- Where the Company engages third parties to Process Data on its behalf, such parties do

- so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organizational measures to ensure the security of any Data.

- The Company endeavors to design its systems and business processes which Process Data to minimise the risks to the privacy, rights and freedoms of employees. This may include carrying out Data Protection Impact Assessments where necessary and maintaining appropriate records of the Processing that the Company carries out.

Employee responsibilities

- Employees may have access to the Data of other employees and of our customers and clients in the course of their employment or contract. Where this is the case, the Company relies on employees to help meet its data protection obligations to staff and to customers and clients.

- Employees must immediately report the discovery of any actual or potential security incident and Data breach (including unauthorised access or disclosure of employee's Data) to Warren.Lynes@onsite-support.co.uk. The Company has an obligation under law to report any Data breach and all employees are expected to assist the Company in complying with its legal reporting obligations. Failure to do so may constitute a disciplinary offence as outlined below.

- Employees who have access to other personal data are required:
  - To access only Data that they have authority to access and only for authorised purposes;

- o Keep and maintain accurate corporate records reflecting our Processing including records of consents from third parties, including customers and clients where relevant.
- o Not to disclose Data except to employees (whether inside or outside the Company) who have appropriate authorisation;
- o To keep Data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- o Not to remove Data, or devices containing Data or that can be used to Data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the Data and/or the device; and
- o Not to store Data on local drives or on personal devices that are used for work purposes.

- Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing or disclosing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

07/01/2026

…………………………………………….. **Date:** …………………………………

Warren Lynes
Managing Director