OT GROUP

Information Security Policy Statement

OT Group Limited ("the Company") is committed to ensuring that the Company maintains and improves information security. This policy has been created to facilitate this and minimise the Company's exposure to such risks.

Policy Statement

- All breaches of information security, whether actual or suspected, will be investigated by the Company. Any investigation will be led by senior IT personnel and an independent Company Director as directed by the CEO or Company Secretary.
- The Company intends to undertake ISO27001 certification for its information systems.
- Information security training will be provided to all Directors and Managers.
- The Company will endeavor to protect all information against unauthorised use.
- Information will be made available to authorised personnel in order to complete their duties.
- Data integrity will be maintained.

OT Group are aware of the importance of managing the risks that unforeseen events can cause the Company.

The Company will ensure that the Compliance Manager operates a Risk Management Document to record all strategic and operational risks the Company is exposed to. The document will record how the Company intends to mitigate these risks. The document is intended to ensure that the Company fully understands the risks it faces and takes adequate precautions to protect all parties who may be affected.

The Group Trading Board will have regard to the risks associated with Company strategy and shall ensure that risks are monitored and remain within an acceptable level.
The Compliance Manager will be responsible for ensuring the day to day maintenance and operation of the Risk Management Document. Significant risks and non-compliance will be reported to the Company Secretary.

Pippa Maynard
Company Secretary

Information Security Policy

Introduction

OT Group is a successful company but is reliant on the information it holds for continued business success. The Company therefore needs to have effective data security measures in place, providing integrity and confidentiality of said data and information systems. In order to achieve effective information security the Company has produced this policy.

The Company Secretary is responsible for all information security policies and ensuring that all Directors and Managers within the business are trained in information security, which should then be discharged to members of their team.

All new employees must be informed of the Information Security Policy and receive training to ensure compliance. This will form part of their induction programme.

Scope

The policy applies to all staff and contractors and any other authorised users. The policy applies to all Company owned information and assets as well as privately owned systems when connected directly or indirectly to the OT Group networks. It includes all Company owned software, data and intellectual property.

Objectives

Primary objectives are:

i. To protect the Company's systems and information from the risks of loss, misuse, damage, abuse and theft. This covers all computers, networking equipment, software, data and all other systems or equipment required to allow OT Group to trade unimpeded.
ii. To make sure all users are aware and comply with all current and relevant polices including legislation that is in force in the UK or EU.
iii. Protect the Company from liability or material effects of misuse of its information systems or data.
iv. Ensure users are aware of their responsibility for protecting the confidentiality and integrity of the data they handle.
v. Ensure all users are aware that the Company will take appropriate action be it disciplinary or legal to protect, recover or claim damages for breach of policy or procedures.

Regulatory Compliance

OT Group will comply with all applicable legislation in force in the UK and EU. The Company Secretary will ensure that the Company keeps up-to-date on legislation and will inform the Compliance Manager where changes to the Information Security Policy are required.

Usage Monitoring

The Company Secretary and certain people in the OT Group IT department are authorised to monitor information systems under their control to ensure compliance. This may include the monitoring of electronic messages including email, instant messaging systems and the like, external communications and external resources such as the World Wide Web.

In order to enforce this policy it is necessary for the Company to use monitoring tools and investigation techniques. This allows OT Group to track and control the use of its networks and systems to detect unauthorised use. The Company can also ensure that network capacity is not compromised by unauthorised use; ensuring bandwidth is maintained for business related data. As a Company, OT Group will be better placed to prevent non compliance, educate, deter and/or detect criminal activity.

The Company may act within the terms of the Regulation of Investigatory Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulation 2000 for the provision of monitoring. This legislation permits that communications may be intercepted in certain circumstances.

Security Breaches

The IT department monitors network activity and responds to alerts and notifications issued by our monitoring solution or any other system generated message. These messages are automatically logged in our central IT Service Desk system. These messages are investigated to ensure information security.

All employees of the Company have a duty to report any breach, likely breach or suspected breach to the IT Service Desk. On receipt of such a report the 1st Line Support Team will escalate to the Support Manager who will in turn inform the Group IT Director and make initial investigations. Any confirmed breach of compliance will be immediately reported to the Company Secretary and the Group IT Director. Both parties must be informed.

On notification the Company may take the required action to prevent further breaches by either disabling the user(s) suspected or any other action deemed reasonable to secure the Company's information.

Any breach of the Company's information systems could lead to loss of data that is protected under UK or EU legislation, such as the Data Protection Act 1998, which may result in the Company being prosecuted. It is essential that all employees who use the information systems of OT Group understand their responsibilities and adhere to this policy.

Policy Awareness and Disciplinary Action

The policy will be published on the Company's Intranet for ease of reference and made available to external sources where such a request is a business requirement. All new employees will have a copy of the policy provided within their starter pack and discussed by their line Manager/Director as part of their induction programme. All current employees will be sent the policy and acceptance will be deemed to have been received unless the employee raises a concern with the Company Secretary.

All contractors will be required to agree to the policy before commencing any work and the policy will be part of the Contractors/Freelance Permit, which allows access to OT Group Systems and Information. Employees may be subject to disciplinary action which may result in dismissal and/or legal action should they fail to comply with this policy. Where a contractor or other third party fails to comply this may result in any contract being terminated without compensation and where appropriate reporting to relevant authorities including the police.

Additional Supporting Polices

All employees and third parties are required to familiarise themselves with other Company related policies as below.

- Data Protection Act 1998 Compliance
- Computer and Internet use policy Information Security Policy Status

This policy does not form part of any employees' contract. It is however a condition of employment that the employee abides by this policy and other policies issued by the Company.

Conditions of Use of OT Group Information Systems

Introduction

This section details the conditions of use of the OT Group Information Systems so that all authorised users of such systems and information are clearly understood.

Conditions of Use

All users of OT Group Information Systems must have first been provided with a unique logon id and password. This is your personal identification and you are required to protect this and are not permitted to share this with anyone, including the IT department.

You should not use another user's id and password to access any systems or attempt to discover another user's id and password. Any attempt to gain access to information that you are not authorised to access is prohibited and could be an offence under the Computer Misuse Act and therefore illegal.

The Company operates a Computer Use and Email Policy and electronic message policy. This is for business use only and should not be used for personal emails. The Company does not allow access to personal email accounts such as Hotmail.

You should not attempt to alter any electronic information that identifies you as the sender of any type of electronic message. This is not acceptable practice and may result in disciplinary action or in some circumstances illegal action.

The Company makes available a wide range of systems for authorised users and therefore access to a wide range of information. A significant amount is available on the internet and World Wide Web. These services are made available to enable you to carry out your duties although the Company does permit private web browsing under certain conditions. All users should ensure that they are aware of the Computer and Internet use Policy.

The Company operate various systems and software to control access to the internet and authorised sites on the World Wide Web. Any attempt to circumvent these will result in disciplinary action and in some circumstances the Company may involve the police.

Usage

The user accepts that:

- Use of the Company's network or any systems including but not limited to wireless, telephone network, laptop, PC, software, data, email, smart phones etc is for the express purpose of work associated with their job role. No system is provided for personal use although the Company may permit personal use at its discretion.

- Any user suspected of breaching the policy agrees that the Company may inspect any system; private or otherwise to establish non-compliance of policy and they will assist in the investigation. Such an inspection will only be carried out after notifying the user.

Compliance

All users must comply with all relevant policies, UK and EU legislation and procedures associated with Information Security.
The following are deemed to be relevant.

- Anti-terrorism, Crime and Security Act 2001
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- UK Data Protection Act 1998
- Freedom of Information Act 2000 and including 6 UK Statutory Instruments and The Freedom of Information (Designation as Public Authorities) Order 2015
- Human Rights Act 1998
- Protection from Harassment Act 1997
- Obscene Publications Act
- Regulation of Investigatory Powers Act 2000
- Telecommunications Act 1984
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000
- The Electronics Signatures Regulations 2002
- The Telecommunications (Data Protection & Privacy, Direct Marketing) Regulations 1999
- Civil Contingencies Act (2004 & 2005) (UK Government)
- Business Continuity Practice Guide: 2006 (UK Tripartite Authorities: Financial Services Authority (FSA), HM Treasury, Bank of England)
- Companies Act 2006 contains a number of provisions concerning records and communications and 46 UK Statutory Instruments including 2 in 2015

- The Privacy and Electronic Communications Regulations 2003

Users must adhere to all terms and conditions of all license agreements including software, equipment and documentation.

Users must not distribute copies of material or software made available to them when using OT Group systems.

Users are responsible for the security of their work and must ensure that such work is made available for the Company's central backup routines. This is to ensure that the Company can recover from disaster events. The Company will not use these backups to restore data accidently deleted by users.

All users of the Company's information systems shall not knowingly or negligently:

- make use of, or access a system for illegal or unauthorised purpose;
- use the Company's systems to store, distribute to other employees or otherwise whether lawful or not that may bring the company into disrepute or damage its reputation;
- attempt to reverse engineer any part of a system or software without written permission of the copyright holder;
- create, store or process or transmit defamatory material or material which is designed or likely to cause harassment, or needless annoyance, inconvenience or anxiety to another be they a user of the Company's systems or not;
- disclose his/her login name/password combination or attempt to access computers or computing services at OT Group or other facilities where express permission has not been granted and therefore access is unauthorised;
- use or produce materials or resources to facilitate unauthorised modification, access, changes, malfunction or access to any OT Group facility;
- display, store or transmit any images or text likely to cause offence e.g. material of a sexual nature, pornographic, sexist, racist, libellous, threatening or defamatory nature;
- forge email signatures and/or headers, imitate and/or forward 'chain' or 'junk' or harassing mail;
- attempt to install unauthorised software on any system without first obtaining permission from the IT department;
- attempt to uninstall/disable or workaround any software or service software with the express permission of the IT Department; or play any unauthorised games

Guidelines for Use of Information System and Services

General

The Company's network and computing systems cover all in house systems, such as databases, MIS, wireless networks, telephony systems and external web servers, email, remote access via VPN, smart phones and laptops. These systems are to be used by authorised users only for the execution of your company duties.

The Company operates software that monitors network usage and details about activity when accessing the World Wide Web. No users should expect privacy regarding use of the internet.

Physical Security

The Company takes security very seriously and has procedures in place to prevent unauthorised access to Company buildings. Users should remain alert to the dangers of strangers in the work place and take steps to prevent the theft of or unauthorised access of information.

No employee or contractor should remove any Company owned equipment or media without the permission of an IT Director, unless such action is part of your authorised job role.
Only equipment owned by the Company should be connected to the Company's network.

Computer System Access

The Company requires all employees to ensure that its systems, data and information is protected from any unauthorised access, accidental or malicious damage at all times.

Active Sessions

Any computer left unattended poses a risk to the business of theft or unauthorised access. All users are expected to take the appropriate action when leaving their device(s) as follows:

- Close down active sessions and log out of the network.
- For temporary departure use, <Windows key> +L to lock the workstation.
- If you are leaving work (home time) you must logout of all systems and shutdown your laptop or PC.

- Mobile phones should be protected by the use of an access code, password, physical ID or pattern.
- Do not store sensitive information on your laptop / smart phone. Information is categorised and where this is of the highest level and is necessary to be stored on a device being removed from the business unit it must be encrypted using the software provided by OT Group.

Password Control

Your password should be created following the controls below

- Minimum length of a password is 8 characters.
- Combination of letters and numbers
- Upper and lower case
- Your account may become locked after 3 unsuccessful attempts

You should not:

- reveal your password to anyone;
- store you password and user id by your workstation; or
- re-use passwords.

You should change your password if you think it has been compromised.

Shared Network resource

The Company provide all users an area for storing information on the Company's network. The Company resources are not infinite and monitoring will be used to highlight users that are approaching acceptable levels of data storage. Users will be advised and expected to remove data (delete) information that is no longer required.

The Company's email system allows for a specific storage amount and this is reviewed on a monthly basis by IT. Users will be advised once they are within 20% of the maximum amount of data permitted and the user will be expected to delete unwanted /old emails. Email is not to be used as a storage for documents, the business provides data storage options for key business documents.

Virus Prevention and Detection

The Company has a number of methods for preventing, identifying and destroying ransomware, viruses and malware that are in circulation. All Company owned PC or MAC based systems are operating McAfee AV which is controlled by McAfee End Point Protection Suite.

Emails are scanned for viruses by our mail supplier and the business operates SPF, DKIM and DMARC, email is quarantined. All users are expected to respond to spam / quarantine email alerts and review accordingly. Extreme caution should be exercised when authorising email to be sent from spam / quarantine. If in doubt users should contact the IT Service Desk.

Users are required to report any ransomware, virus or malware suspicion/alert to the IT Service Desk immediately.

All users are asked to ensure that Anti-Virus is installed and operational, error messages should be reported to the IT Service Desk immediately

All users should not use CD ROMs, Memory sticks, floppy disks or other media that has been used on other non OT Group systems. This includes media used on home equipment or third party equipment without said media being scanned by IT prior to every use. The Company will enforce encryption on removal media and private information may be lost and unrecoverable.

Laptops, Wireless Networks and VPN, Private storage.

The Company provides mobile equipment to employees for the sole purpose of carrying out their duties. These devices are capable of wireless networking and remote connection to the OT Group systems. The Company needs to minimise the risk of such connections and not all users will be granted such access.

Laptops

Only Company owned laptops are allowed to connect to the Company's networks. Therefore private or third party equipment will not be permitted to have the Company's security keys, VPN software or other software licensed to the business.
Laptops are to be used solely for business purposes and private use is not permitted.

Wireless

The Company operate three wireless networks, two internal networks separating office traffic from warehouse traffic. This is for performance and BCP reasons. A third GUEST network is available. All systems use WPA2 Enterprise encryption and authentication is via the company's AD server. Access is further restricted as below.

- Equipment must be company owned, unless joining the Guest network.
- Only the GUEST network broadcasts.
- Guest sign on is available by request to the IT Service Desk. This will allow access to the Internet only via OT web proxy using Company policy based controls for content and type.

Private Storage

The Company does not permit the use of business equipment, either laptop, PC, smart phone etc as this may hinder any recovery or deployment of systems. Therefore users should not store private information as the Company accepts no liability for the destruction, loss of said data.