Company Name:	Twenty-Four Seven Recruitment Services Ltd					
Policy Name:	IT Data Security Policy					
Review Date:	V1 undated	V2 30/03/22				
Reviewed and authorised by:	Amanda Lillis – Hr Director					

Policy Statement

The purpose of this Policy is to establish a framework for managing risks and protecting the Company's IT infrastructure, computing environment, hardware, software and any and all other relevant equipment ("IT Systems") against all types of threats, internal or external, intentional or unintentional.

Responsibilities

The IT department shall be responsible for carrying out the installation, ongoing maintenance (including without limitation, any upgrades or repairs) and ensuring the security and integrity of the IT Systems, either directly or, via an authorised third party. Accordingly, the IT Department is responsible for data stored on the IT system unless otherwise stated.

In furtherance of above, the IT Department shall be responsible for:

(a) investigating any security breaches and / or misconduct, and shall escalate to James Ritchie and/or Amanda Lillis as appropriate;

(b) regularly reviewing IT security standards within the Company and ensuring the effective implementation of such standards, by way of periodic audits and risk assessments, with regular reports being made to the Company's internal senior management who shall be responsible on the condition of the Company's information security and compliance with this Policy;

(c) providing adequate support in relation to IT security matters and use of the IT Systems, to all Users;

(d) ensuring that the access to IT Systems granted to all Users takes into account their job role, responsibilities and any additional security requirements, so that only necessary access is granted for each User;

(e) dealing with all reports, whether from Users or otherwise, relating to IT security matters and carrying out a suitable response for the situation;

(f) implementing appropriate password controls, as further detailed below;

(g) maintaining a complete list of all hardware items within the IT Systems. All such hardware shall be labelled, and the corresponding data shall be kept by the IT Department; and,

(h) ensuring that daily backups of all data stored within the IT Systems are taken, and that all such backups are stored off the Company premises at a suitably secure location.

The Users shall be responsible for:

(a) informing the IT Department immediately of any actual or potential security breaches or concerns relating to the IT Systems;

Registered Office: Oakwood House, Blackwood Business Park, Ash Road South, Wrexham Industrial Estate, Wrexham, LL13 9UG
Telephone 01978 664195 Fax 01978 661065 Email enquiries@24-7recruitment.net www.24-7recruitment.net
Reg No:4083397 VAT No: 762741618

(b) informing the IT Department immediately in respect of any technical or functional errors experienced relating to the IT Systems; and,

(c) complying with this Policy and all laws applicable to the Users relating to their use of the IT Systems.

Users must not attempt to resolve an IT security breach on their own without consulting the IT Department first.

Scope

This policy applies to all employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, casual workers and agency staff, or any other person associated with us, or any of our subsidiaries or their employees, wherever located (collectively referred to as **users** in this policy). This policy covers all users of 24-7 Recruitments IT Systems.

Policy

Access to IT Systems

There shall be logical access controls designed to manage electronic access to data and IT System functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all Users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

All IT Systems shall only be accessible by a secure log-in system as deemed suitable by the IT Department. Such suitable systems may include, without limitation, secure passwords, fingerprint identification and facial recognition.

The IT Department shall conduct regular system audits or event logging and related monitoring procedures to proactively record User access and activity on the IT Systems for routine review.

IT Systems that are not intended to be part of everyday use by most Users (including without limitation, servers, networking equipment and infrastructure) and any other areas where personal data may be stored (e.g. data centre or server room facilities) shall be designed to:

(a) protect information and physical assets from unauthorised physical access;
(b) manage, monitor, and log movement of persons into and out of the relevant facilities; and
(c) guard against environmental hazards such as heat, fire, and water damage.

Passwords

The IT Department shall implement password controls designed to manage and control password strength, expiration and usage including prohibiting Users from sharing passwords and requiring that the Company passwords that are assigned to Users:

(a) be at least 6 characters in length,
(b) not be stored in readable format on the Company's IT Systems; and,
(c) must have defined complexity.

Users must keep passwords confidential and not share it with anyone else. Individual user accounts are for the use of the assigned individual only and must not be shared.

Hardware

All Company mobile devices (including, without limitation, laptops, tablets and mobile telephones) should be kept securely by Users using secure cases where appropriate. Users should not leave such mobile devices unattended other than at their homes or secure Company premises.

Registered Office: Oakwood House, Blackwood Business Park, Ash Road South, Wrexham Industrial Estate, Wrexham, LL13 9UG
Telephone 01978 664195 Fax 01978 661065 Email enquiries@24-7recruitment.net www.24-7recruitment.net
Reg No:4083397 VAT No: 762741618

All Company non-mobile devices (including, without limitation, desktop computers, workstations, and monitors) shall, wherever possible and practical, be secured when not in use and should not be left unattended in public locations.

Users are not permitted to connect any of their personal hardware to the IT Systems without the express approval of the IT Department.

Software

All software installation on to the IT Systems shall be the responsibility of the IT Department. Users are not permitted to install any software on to the IT Systems unless expressly approved in writing by the IT Department.

All software installed on to the IT Systems shall be kept sufficiently up to date in order to ensure that the security and integrity of the IT Systems is not compromised.

Vulnerability Assessment and Anti-Virus

The IT Department shall carry out regular vulnerability assessments, and utilise patch management, threat protection technologies and scheduled monitoring to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

The IT Department shall ensure that the Company uses an up-to-date reputable anti-virus checking software tool to check the IT Systems and to scan all email attachments before they are opened.

Users may download files from any cloud storage systems, subject to prior approval from the IT Department; and Users shall permit any such files to be scanned for viruses as part of the download process.

The IT Department shall implement network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

Data Protection

The collection, holding and processing of all personal data (as defined in the General Data Protection Regulation 2016 ("GDPR")) by the Company will be carried out in compliance with (i) the GDPR and (ii) the Company's own Data Protection Policy.

The IT Department shall ensure there are data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for personal data that is:

(a) transmitted over public networks (i.e., the Internet) or when transmitted wirelessly; or
(b) at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).

All emails containing personal data must be encrypted.

Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of

Registered Office: Oakwood House, Blackwood Business Park, Ash Road South, Wrexham Industrial Estate, Wrexham, LL13 9UG
Telephone 01978 664195 Fax 01978 661065 Email enquiries@24-7recruitment.net www.24-7recruitment.net
Reg No:4083397 VAT No: 762741618

GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

The IT Department shall ensure operational procedures and controls to provide to provide for the secure disposal of any part of the IT Systems or any media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Company's possession.

Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.

All personal data stored electronically should be backed up daily with backups stored onsite AND/OR offsite. All backups should be encrypted.

All electronic copies of personal data should be stored securely using passwords and data encryption.

Only Users that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.

All Users that have access to, and handle personal data on the Company's behalf, shall adhere to the Company's Data Protection Policy.

Business Continuity

The Company shall have in place adequate business resiliency/continuity and disaster recovery procedures designed to maintain any information and the supply of any service and/or recovery from foreseeable emergency situations or disasters. Please Business Continuity Policy and Business Continuity Plan.

Email and Internet

Please refer to the Company's policy on Email and Internet usage in respect of email and internet use on the IT Systems.

Clean Desk Policy

Please refer to the Company's Clean Desk Policy in respect of securing end user workspace.

Training and communication

Training on this policy should form part of the induction process for all new employees. All existing employees should receive relevant training on how to adhere to this policy.

Non compliance

A breach of any of the provisions of this Policy by any Relevant Person of the Company will constitute a disciplinary offence and will be dealt with in accordance with the Company's disciplinary procedure. Depending on the gravity of the offence, it may be treated as gross misconduct and could render the employee liable to summary dismissal without payment of notice.

Breach of this policy by any Relevant Person who is a temporary worker, contractor or consultant providing his/her services to the Company may lead to the immediate termination of that temporary workers, contractor's, or consultant's engagement by the Company.

Registered Office: Oakwood House, Blackwood Business Park, Ash Road South, Wrexham Industrial Estate, Wrexham, LL13 9UG
Telephone 01978 664195 Fax 01978 661065 Email enquiries@24-7recruitment.net www.24-7recruitment.net
Reg No:4083397 VAT No: 762741618