1.0 Purpose

The use of computer systems and the exchange of information electronically have increased rapidly in the area of training. Within Team LM there is a growing reliance on computer systems to expand communications, and improve management and control. This growing dependence comes at a time when the number of threats and actual attacks on these computer systems is constantly increasing.

Information is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and properly protected information is essential to the successful operation of Team LM in the provision of services to our customers.

The purpose of this Information Security Policy and its supporting policies, standards and guidelines is to define the security controls necessary to safeguard Team LM information systems and ensure the security, confidentiality, availability and integrity of the information held therein.

This policy is mandatory and by accessing any information or Information Technology (IT) resources which are owned or leased by Team LM, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy is authorised by Team LM Senior Management Team and represents Team LM's national position. The policy takes precedence over all other relevant policies which may have been developed at a local level.

This policy applies to all Team LM staff, contractors, sub-contractors and authorized third party commercial service providers that use the organizations I.T. resources and/or process information on behalf of Team LM.

3.0 Legislation

Team LM has an obligation to abide by all relevant Irish legislation and European legislation. The relevant acts, which apply in Irish law to Information Systems, include but are not limited to:

- *The Data Protection Act (2018)*
-

4.0 Definitions

A list of terms used throughout this policy are defined in *appendix A.*

5.0 Policy

It is the policy of Team LM to: -

- Implement human, organisational, and technological security controls to preserve the confidentiality, availability and integrity of its information systems and the information held therein;

- Develop and maintain appropriate policies, procedures and guidelines to effect a high standard of information technology security, reflecting industry best practice;

- Monitor, record and log all activity on Team LM network and use of its information technology resources

- Comprehensively assess and manage risks to Team LM information systems and the information held therein;

- Continuously review and improve Team LM information technology security controls, and rapidly determine the cause of any breach of security and minimize damage to information systems should any such incident occur;

- Comply with all laws and regulations governing information technology security;

- Establish information technology security education and awareness initiatives within Team LM.

6.0 Supporting Policies, Standards and Guidelines

There are a number of supporting Team LM policies, standards and guidelines to accompany this policy document. Each of these accompanying policies, standards and guidelines is published on the Team LM intranet and covers a specific area of information security.

All Team LM staff, contractors, sub-contractors and third party commercial service providers authorised to use Team LM's Information Technology (I.T.) resources are required to familiarise themselves with these accompanying policies, standards and guidelines and to work in accordance with them.

The following is a list of the accompanying policies, standards and guidelines.

6.1 Information Technology (I.T.) Acceptable Use Policy

The *Information Technology Acceptable Use Policy* outlines the correct and proper manner in which Team LM's Information Technology (I.T.) resources are to be used. It covers the following areas:

- The use of computer accounts and passwords;
- Confidentiality and privacy of information;
- The use of computer hardware and software;
- The use of laptop computers and other mobile computer devices;
- The security of Team LM information, systems and computer devices;
- Lost, stolen and damaged computer devices;
- The use of the Team LM telephone system;
- Storage of information;
- Backup of information;
- Security of information;
- Transfer and transport of information;
- Disposal of information;
- Tele-working / home-working;
- Virus & Malicious Software Protection
- The unacceptable use of Team LM information technology resources

6.2 Email Policy

The *Email Policy* outlines the correct and proper manner in which the Team LM's Email and Internet facilities are to be used. It covers the following areas:

- The confidentiality and privacy of email messages;
- The use of the Team LM email and internet facilities;
- The transmission of confidential or personal information via email and internet;
- The legal status of Team LM email messages;
- The use and ownership of Team LM email accounts;
- The use of third party and web based email facilities;
- Access to restricted and blocked internet content;
- The installation or use of third party internet facilities;
- The unacceptable use of Team LM email and internet facilities.

6.3 Password Standards Policy

The *Password Standards Policy* outlines the standard for the creation and use of secure passwords for use on the Team LM's Information Technology (IT) resources. It covers the following areas:

- The creation of secure passwords;
- Minimum password length;
- Composition and complexity of passwords;
- The use and security of passwords.

6.4 Encryption Policy

The *Encryption Policy* outlines the acceptable use and management of encryption software throughout Team LM. It covers the following areas:

- Minimum level of encryption;
- Approved Encryption Algorithms and Protocols;
- Encryption of Team LM computer devices;
- Encryption of Team LM storage devices;
- Encryption of Team LM email and internet messages and traffic;
- Encryption of Team LM wireless network traffic.

6.5 Remote Access Policy

There is no remote access capability as all information is held within the Team LM main office.

6.6 Mobile Phone Device Policy

There are no mobile phones provided to the staff of Team LM.

6.7 Information Classification & Handling Policy

The *Data Classification & Handling Policy* outlines how Team LM information must be classified and handled according to its sensitivity. It covers the following areas:

- The different classifications of Team LM Information;
- How each class of information should be handled and processed;

6.8 Data Breach Handling Procedure

The *Data Breach Handling Procedure* outlines the approved management approach to be followed in the event of a Team LM data protection breach. It covers the following areas:

- Identification and classification of a breach;
- Containment and recovery;
- Risk assessment;
- Notification of a breach;
- Evaluation and response.

6.9 Service Provider Confidentiality Agreement

There are no service providers currently processing data on behalf of Team LM.

7.0 Roles & Responsibilities

List various groups/departments and what their responsibilities are

7.1 Board of Directors

The Board of Directors in Team LM is responsible for:

- Approving and publishing the policy;
- The annual review of policy;
- Approving all changes and amendments to the policy.

7.2 IT Service Provider

The IT Service Provider is responsible for:

- The identification, implementation and management of appropriate security controls necessary to safeguard Team LM's network (LAN/WAN) and supporting infrastructure;
- The implementation of system-level security controls as defined by the information owner or the CEO;
- The provision of facilities for information backups on network file servers and other centralized information stores but excluding backups of the hard disks on individual computers;
- The provision of services which enable authorised user's access to appropriate electronic information systems and data;
- Liaising with and advising Team LM management, individual users and line managers on the appropriate actions to take in the event of an actual or suspected breach data security.

7.3 Senior Management team

Senior Management team are responsible for:

- The implementation of this policy and all other relevant Team LM policies within the business areas for which they are responsible;
- Consulting with the HR Department in relation to the appropriate procedures to follow when a breach of this policy has occurred;
- Consulting with the IT Service Provider in relation to the appropriate actions to be taken when an actual or suspected breach of data security has occurred.

7.4 Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant Team LM policies, procedures, regulations and applicable legislation;
- Respecting and protecting the privacy and confidentiality of the information they process at all times;
- Complying with instructions issued by the IT Service Provider on behalf of Team LM;
- Reporting all misuse and breaches of this policy to the senior management team immediately;
- Reporting all actual or suspected breaches of data security to the Data Protection Administrator and IT Service Provider immediately.

7.5 Data Protection Administrator

The Data Protection Administrator are responsible for:

- Providing training and advice on data protection;
- Liaising with and advising the Team LM management, individual users and line managers on the appropriate actions to take in the event of an actual or suspected breach data security.

8.0 Policy Distribution & Awareness

- This policy and its supporting policies, standards and guidelines will be published on the Team LM Network drive. Hard copies of the policy and its supporting policies, standards and guidelines will be available on request from the Data Protection Administrator.

- The Board of Directors may make periodic policy announcements by email.

- Team LM Senior Management Team will ensure that all existing and new staff, contractors, subcontractors and third party commercial service providers who report to them are made aware of and have access to the policy and its supporting policies, standards and guidelines.

- Data Protection training which also covers large sections of this policy and its supporting policies, standards and guidelines will be available from Team LM's Data Protection Administrator.

9.0 Review & Update

- This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to Team LM's organisation structure and business practices are properly reflected in the policy.

- Updates to the policy and the supporting policies, standards and guidelines will be made periodically and will be posted on Team LM network drive and/or announced by email.

- The most up to date version of this policy is published on the Team LM network drive.

10.0 Breaches of Security

- For security and technical reasons Team LM reserves the right to monitor, record and log all use of its information technology resources and activity on Team LM network.

- Any individual suspecting that there has been, or is likely to be a breach of data security must inform their line manager, the Data Protection Administrator and their IT Service Provider immediately. The IT Service Provider and Data Protection Administrator will advise the individual on what action should be taken.

- Team LM reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. Team LM staff, contractors or sub-contractors who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in Team LM disciplinary procedures.

Appendix A

Authorisation / Authorised: Official Team LM approval and permission to perform a particular task.

Availability: Ensuring that authorized users have access to information and associated assets whenever required.

Breach of Data Security: The situation where Team LM confidential or restricted data has been put at risk of unauthorized disclosure as a result of the loss or theft of the data or, the loss or theft of a computer or storage device containing a copy of the data or through the accidental or deliberate release of the data.

Confidentiality: Ensuring that information is only accessible to those users who are authorized to access the information.

Team LM Network: The data communication system that interconnects different wired and wireless Team LM Local Area Networks (LAN) and Wide Area Networks (WAN).

Team LM Network Server: A computer on Team LM network used to manage network resources.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by Team LM.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Security: The preservation of confidentiality, integrity and availability of information.

Information System: A computerized system or software application used to access, record, store, gather and process information.

Integrity: Ensuring the accuracy and completeness of information and associated processing methods.

IT Service Provider: An outsourced specialist in IT Infrastructure management who is responsible for maintaining system availability, integrity and confidentiality.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- Obtaining, recording or keeping the information;
- Collecting, organising, storing, altering or adapting the information;
- Retrieving, consulting or using the information;
- Disclosing the information or data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the information.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Senior Management Team: The team responsible for the day-to-day managing of the company.

Third Party Service Provider: Any individual or commercial company that have been contracted by Team LM to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services etc.) to Team LM.

Threat: A potential cause of an incident that may result in harm to a system or organisation.

Users: Any individual using any of Team LM's I.T. resources.