Data Encryption Policy

Purpose

The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout Riverside Training

This policy is mandatory and by accessing any Information Technology (I.T.) resources which are owned or leased by Riverside Training, users are agreeing to abide by the terms of this policy.

Scope

- All I.T. resources provided by Riverside Training;
- All users (including staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of Riverside Training's I.T resources;
- All connections to (locally or remotely) Riverside Trainings network Domains
- (LAN/WAN/WiFi);
- All connections made to external networks through Riverside Training network..

Principles of Encryption

Where possible all confidential and restricted information must be stored on a secure Riverside Training network server with restricted access. Where it has been deemed necessary by a line manger to store confidential or restricted information on any device other than a Riverside Training network server the information must be encrypted.

All confidential and restricted information transmitted via email to an email address outside of Riverside Training domain (i.e. one that does not end in "@riverside-training.co.uk") must be encrypted.

Desktop Computers

All desktop computers will contain password protected access to the shared drive. Passwords should not be shared by individuals and staff should ensure that desktops are closed down or locked before leaving them.

Laptop, Mobile Computer & Smart Devices

The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential and restricted information.

Removable Storage Devices

All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.

The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removal storage device.

USB Memory Sticks

Confidential and restricted information may only be stored on Riverside Training approved encrypted USB memory sticks which are available from Business Support Team.

The storage of confidential or restricted information on any other USB memory sticks (encrypted or otherwise) will be considered a breach of this policy.

Riverside Training approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential or restricted information. They must not be used for the long term storage of confidential or restricted information, which must where possible be stored on a secure Company network server.

Confidential and restricted information stored on Riverside Training approved USB memory stick must not be transferred to any internal (except a secure Company network server) or external system in an unencrypted form.

Transmission Security

All confidential or restricted information transmitted through email to an email address outside of Riverside Training domain (i.e. one that does not end in "@riverside-training.co.uk") must be encrypted. The transfer of such information outside of Riverside Training domain must be authorised by a Riverside Training line manager and comply with GDPR. The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channels (for example: Secure FTP, TLS, VPN etc.). The transfer must be authorised by a Riverside Training line manager. The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

Roles & Responsibilities

The Senior Management Team is responsible for:

- The selection and procurement of all encryption facilities used within Riverside Training.
- The provision, deployment and management of encryption facilities within the Company.
- The provision of training, advice and guidance on the use of encryption facilities within Riverside Training;

Information Owners

Information owners are responsible for:

- The implementation of this policy and all other relevant policies within Riverside Training or service they manage;

- The ownership, management, control and security of the information processed on behalf of Riverside Training;
- The ownership, management, control and security of information systems used on behalf of Riverside Training;
- Maintaining a list of information systems and applications which are managed and controlled by the Company.
- Making sure adequate procedures are implemented to ensure compliance of this policy and all other relevant policies;

Users

Each user of Riverside Training's IT resources is responsible for:

- Complying with the terms of this policy and all other relevant Riverside Training 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 Business Support Team on behalf of Riverside Training.
- Ensuring all encryption passwords assigned to them are kept confidential at all times and not shared with others;
- Ensuring encryption passwords used to access encrypted devices are not written down on the encrypted device or stored with or near the encrypted device;
- Reporting all misuse and breaches of this policy to their line manager.

Review
This policy will be reviewed on an annual basis