Status: Approved
Version: 1
Reviewed: May 2018

Introduction

This policy is concerned with the management and security of Elliott Training's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to Elliott Training Ltd. and the use made of these assets by its employees and others who may legitimately process information on behalf of the company.

PURPOSE

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

Scope

The documents in the Information Security Policy set apply to all information assets which are owned by Elliott Training Limited, used by the company for business purposes or which are connected to any networks managed by the company.

The documents in the Information Security Policy set apply to all information which Elliott training Limited processes, irrespective of ownership or form.

The Information Security Policy applies to all employees of Elliott Training and any others who may process information on behalf of Elliott Training Limited.

Index

1. Compliance

Contents

Introduction

This Compliance Policy outlines Elliott Training Limited requirements to comply with certain legal and regulatory frameworks.

Compliance with legislation

Elliott Training Limited provides policy statements and guidance for staff in relation to compliance with relevant legislation to help prevent breaches of Elliott Training legal obligations. However, individuals are ultimately responsible for ensuring that they do not breach legal requirements during the course of their work.

Users of online or network services are individually responsible for their activity and must be aware of the relevant legal requirements when using such services. Elliott Training Limited must comply with all relevant legal requirements whether such requirements are detailed in internal policies or not. Any suspected breach of the legal requirements must be reported.

Software licence management

All software used for the business must be appropriately licensed. Elliott Training Limited must comply with the software and data licensing agreements it has entered into. During the negotiation process of such agreements, full consideration must be given to how compliance with the agreement can practically be achieved.

Third party terms and conditions

Where Elliott Training uses the services of a third party provider, staff will also be subject to their terms and conditions in so far as they relate to information security.

Compliance with the Information Security Policy

Elliott Training Limited own information security policies must be adhered to at all times when handling company information and business must ensure it is acting legally when operating such policies. All staff and other persons who may handle business information must be made aware of Elliott Training information security policies and of any amendments made to them. Individuals must also confirm that they have read and understood these policies and how they apply to the information they handle.

Records management

Elliott Training is required to retain certain information, whether held in hard copy or electronically, for legally defined periods. Such information must be appropriately safeguarded and not destroyed prior to the defined minimum retention period, while remaining accessible to those who require access and are authorised to access that information. In accordance with the Data Protection Act, personal data should not be retained for longer than it is required for the purposes for which it was collected.

2. User Management

Contents

Introduction

This User Management Policy sets out the requirements for the effective management of user accounts and access rights. This management is essential in order to ensure that access to Elliott Training information and information systems is restricted to authorised users.

Scope

All information systems used to conduct Elliott Training business, or which are connected to the companies' network must be managed in accordance with this policy.

Eligibility

User accounts will only be provided for:

- Current staff
- Guests or contractors of Elliott Training who may be granted temporary access to the company's network.

Authorisation to manage

The management of user accounts and privileges on information systems is restricted to suitably trained and authorised members of staff.

Account and privilege management

Accounts will only be issued to those who are eligible for an account and whose identity has been verified. When an account is created, a unique identifier (userID) will be assigned to the individual user for his or her individual use. This userID may not be assigned to any other person at any time (userIDs will not be recycled). On issue of account credentials, users must be informed of the requirement to comply with the Information Security policy.

Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles. Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. when a member of staff changes their role or a member of staff or leaves the business).

Privileged accounts are accounts used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

Password management

Passwords for new employees will be set by the new employee on starting. Exceptionally, the new member may be informed of an initial, temporary password, which must be communicated in a secure way and must be changed by the new employee immediately. This change should be enforced automatically wherever possible.

3. Acceptable Use

Contents

Introduction

This Acceptable Use Policy sets out the responsibilities and required behaviour of users of the company's information systems, networks and computers.

Scope

All employees, visitors and guests of Elliott Training who have been granted access to use the companies facilities together with any others who may have been granted permission to use the companies' information and communication technology facilities are subject to this policy.

User identification and authentication

Each member will be assigned a unique identifier (userID) for his or her individual use. This userID may not be used by anyone other than the individual user to whom it has been issued. Each member will be assigned an associated account password which must not be divulged to anyone, including IT Services staff, for any reason.

This password should not be used as the password for any other service. Individual members are expected to remember their password and to change it if there is any suspicion that it may have been compromised.

Each employee will also be assigned a unique email address for his or her individual use and some employees may also be given authorisation to use one or more generic (role based) email addresses.

Employees must not use Elliott Training email address assigned to anyone else without their explicit permission. Email addresses are Elliott Training owned assets and any use of these email addresses is subject to Elliott Training policies.

Personal use of facilities

Company information and communication facilities, including email addresses and computers, are provided for purposes related to work Elliott Training Limited. Very occasional personal use is permitted but only so long as:

- it does not interfere with the member of staff's work
- it does not contravene any Elliott Training
- it is not excessive in its use of resources

Elliott Training facilities should not be used for the storage of data unrelated to the business of Elliott Training Limited. In particular, facilities should not be used to store copies of personal photographs, music collections or personal emails. Employees should not use a personal email account to conduct Elliott Training business and should maintain a separate, personal email account for personal email correspondence. All use of company information and communication facilities, including any personal use is subject to Elliott Training policies.

Connecting devices to Elliott Training networks

In order to reduce risks of malware infection and propagation, risks of network disruption, it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose.

To further reduce risk of data loss, members of staff should not connect any personally owned peripheral device which is capable of storing data (for example, a personally owned USB stick) to any Elliott Training owned equipment, irrespective of where the equipment is located.

Any device connected to a company network must be managed effectively. Devices which are not are liable to physical or logical disconnection from the network without notice.

Use of services provided by third parties

Wherever possible, staff should only use services provided or endorsed by the business for conducting Elliott Training business.

Unattended equipment

Computers and other equipment used to access company facilities must not be left unattended and unlocked if logged in. Employees must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended. Particular care should be taken to ensure the physical security of all equipment when in transit.

Unacceptable use

In addition to what has already been written above, the following are also considered to be unacceptable uses of company facilities.

- Any illegal activity or activity which breaches any company policies.
- Any attempt to undermine the security of the company's facilities. (For the avoidance of doubt, this includes undertaking any unauthorised penetration testing or vulnerability scanning of any systems.)
- Providing access to facilities or information to those who are not entitled to access.

- Any irresponsible or reckless handling or unauthorised use of data (see the Information Handling section).
- Any use which brings Elliott Training into disrepute.
- Any use of company's facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- Sending unsolicited and unauthorised bulk email (spam) which is unrelated to the legitimate business.
- Creating, storing or transmitting any material which infringes copyright.
- Creating, storing or transmitting defamatory or obscene material.
- Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of Elliott Training facilities.
- Failing to report any breach, or suspected breach of information security to Sarah Elliott.
- Failing to comply with a request from an authorised person for you to change your password.

Penalties for misuse

Minor breaches of policy will be dealt with by Sarah Elliott. More serious breaches of policy (or repeated minor breaches) will be dealt with under the Elliott Training disciplinary procedures. Where appropriate, breaches of the law will be reported to the police.

4. Information handling Policy

Contents

Introduction

Information assets must be managed to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

Inventory and ownership of information assets

An inventory of the company's main information assets will be developed and maintained and the ownership of each asset kept by Sarah Elliott. Each asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

Access to information

Employees of Elliott Training will be granted access to the information they need in order to fulfil their roles within the business. Employee's who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

Disposal of information

Great care needs to be taken to ensure that information assets are disposed of securely. Confidential paper waste must be disposed of in accordance in a secure manor.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of Elliott Training, unless the disposal is undertaken under contract by an approved contractor.

In cases where a storage system (for example a computer disc) is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. If this is not possible, then the storage system should not be returned to the supplier and should remain in the possession of Elliott Training until it is disposed of securely.

Removal of information

Elliott Training data which is subject to the Data Protection Act or GDPR Regulations which has a classification of confidential should be stored using company facilities or with third parties subject to a formal, written legal contract, wherever possible. In cases where it is necessary to otherwise remove data from the business, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. Confidential data in electronic form must be strongly encrypted prior to removal. Particular care needs to be taken when information assets are in transit. Company supplied mobile devices must always be fully encrypted.

Using personally owned devices

Any processing or storage of company information using personally owned devices must be in compliance with the companies' s Mobile and Remote Working Policy (see below).

Information on desks, screens and printers

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times. Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

Backups

Sarah Elliott will ensure that appropriate backup and system recovery measures are in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.

Exchanges of information

Whenever significant amounts of personal data or other confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.

Information classified as confidential may only be exchanged electronically both within Elliott Training and in exchanges with third parties if the information is strongly encrypted prior to exchange. Hard copies of information classified as confidential or above must only be exchanged with third parties via secure (for example, special) delivery.

When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.

Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.

Employees must not disclose nor copy any information classified as confidential unless they are authorised to do so.

Reporting losses

All employees have a duty to report the loss, suspected loss or unauthorised disclosure of any company information asset to the Sarah Elliott.

5. System Management

Contents

Introduction

This System Management Policy sets out the responsibilities and required behaviour of those who manage computer systems on behalf of Elliott Training Limited.

Scope

Elliott Training computer systems will be managed by suitably skilled staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability).

Duties and responsibilities

Sarah Elliott is system manager and is in a uniquely privileged position and plays a key role in ensuring the security of the company's systems and services.

System managers are responsible for ensuring appropriate business continuity measures are in place to protect against events which might otherwise result in loss of service. They should also assign (and record) a confidentiality level to their systems which indicates the suitability, or otherwise, of using any individual system for the storage or processing of different categories of company data (see the Information Handling section). This is to allow data owners to make informed decisions as to whether the system meets their security requirements.

System managers are also responsible for ensuring the on-going security of their systems and must apply software patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches must be applied in accordance with software suppliers' recommendations (or requirements) or within 5 working days of release, whichever is the shorter. If it is not possible to patch within this time, other compensatory control measures must be taken to mitigate risk.

Employees are authorised to act promptly to protect the security of their systems, but must be proportionate in the actions that they take, particularly when undertaking actions which have a direct impact on the users of their systems.

System managers must immediately report any information security incidents to Operations Manager.

Change management

All changes to computer systems are subject to IT Services' established change management processes and procedures. File integrity monitoring software should be used to help detect unauthorised system changes.

Access control

Access to all computer systems must be via a secure authentication process (domain managed accounts), with the exception of read-only access to publicly available information. Locally administered accounts should be avoided wherever possible.

Access must only be granted in strict accordance with the User Management policy.

Administrator accounts and accounts with elevated privileges must only be used when necessary to undertake specific tasks which require the use of these accounts. At all other times, the principle of "least privilege" should be followed.

Access to administrator accounts should be protected by two-factor authentication wherever possible.

Monitoring and logging

The use and attempted use of all computer systems should be logged. The data logged should be sufficient to support the security, compliance and capacity planning requirements of the system but should not be unnecessarily intrusive.

Users of systems should be given clear information of what information is recorded, the purposes of the recordings and the retention schedule of the data collected. This information should be made available to users in the form of a system specific privacy policy.

The Data Protection Act/ GDPR Regulations requires that any personal data collected is collected for specific purposes and that it should be deleted when it is no longer needed.

It is recommended that log files are recorded on a different system from the system being monitored.

Audit logs should be configured to record any actions undertaken using administrator or elevated privileges. Audit logs should be secured to protect them from unauthorised modification.

Vulnerability scanning

All systems may be subject to vulnerability scans. These scans may be undertaken by appropriately skilled staff or by approved external assessors.

System clocks

All system clocks must be synchronised to reliable time sources.

6. Network Management

Contents

Introduction

This Network Management Policy sets out the responsibilities and required behaviour of those who manage communications networks on behalf of Elliott Training Limited.

Scope

All of the Elliott Training communications networks, whether wired or wireless are in scope, irrespective of the nature of the traffic carried over the networks (data or voice).

Management of the Network

The company's communications networks will be managed by suitably skilled staff to oversee their day-to-day running and to ensure their on-going security (confidentiality, integrity and availability).

Network staff are in highly privileged positions and play a key role in contributing to the security of the company's information assets. They are expected to be aware of the Information Security policy in its entirety and must always abide by the policy. Network staff are authorised to act promptly to protect the security of their networks, but must be proportionate in the actions which they take, particularly when undertaking actions which have a direct impact on the users of the network.

Network staff must immediately report any information security incidents to the Operations Manager.

Network Design and Configuration

The network must be designed and configured to deliver high levels of performance, availability and reliability, appropriate to the business needs, whilst providing a high degree of control over access to the network. The network must be segregated into separate logical domains with routing and access controls operating between the domains to prevent unauthorised access to network resources and unnecessary traffic flows between the domains.

Physical Security and Integrity

Networking and communications facilities, including wiring closets, data centres and computer rooms must be adequately protected against accidental damage (fire or flood, for example), theft, or other malicious acts. The network should, where appropriate and possible, be resilient to help mitigate the impact of the failure of network components.

Change Management

All changes to network components (routers, firewalls etc) are subject to IT Services' established change management processes and procedures.

Connecting Devices to the Network

It is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the company's guest wireless networks.

Any device connected to a company network must be managed effectively. Devices which are not are liable to physical or logical disconnection from the network without notice.

All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing, in accordance with normal operational practices.

Access Controls

Access to network resources must be strictly controlled to prevent unauthorised access. Access control procedures must provide adequate safeguards through robust identification and authentication techniques.

7. Software Management

Contents

Introduction

This Software Management Policy sets out the principles and expectations for the security aspects of managing software by IT staff and end users where relevant

General software management principles

All software, including operating systems and applications must be actively managed.

Those responsible for software must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

Software managers are responsible for ensuring the on-going security of their software and must apply security patches in a timely manner (depending on the criticality rating of the vulnerabilities addressed by the patches and the level of exposure to the vulnerabilities). High priority patches should either be applied within 5 working days of release or other compensatory control measures taken to mitigate risk.

Staff involved in managing or developing software must be suitably skilled.

Software procurement

When business requirements for new systems or enhancements are being specified, the specification documents should describe any special or essential requirements for security controls. These could include manual controls required during operation.

When software for use by the company is being procured, there must be an assessment of whether the software incorporates adequate security controls for its intended purpose. It must be investigated and considered whether proposed new software or upgrades are known to have outstanding security vulnerabilities or issues.

At the time of software procurement, the basis of future support and the expected supported lifetime of the product should be established. It may be important to have assurance that manufacturers will provide updates to correct any serious security vulnerabilities discovered in the future.

Software installation

Checks should always be made that there is a valid licence before installing software and users advised of any special conditions regarding its usage. Automated installs should be used wherever possible.

Software must not be put into user service on systems unless a department or group has assessed and committed to providing sufficient resourcing for its ongoing management. Appropriate assessment / tests should be made to avoid new software causing operational problems to other systems on the network.

Software regulation

Use or installation of unlicensed software and using software for illegal activities could be construed to be a disciplinary offence.

Use of software which tests or attempts to compromise company system or network security is prohibited unless authorised by the CEO.

Use of software which causes operational problems that inconvenience others, or which makes demands on resources which are excessive or cannot be justified, may be prohibited or regulated.

Software found on company systems which incorporates malware of any type is liable to automated or manual removal or deactivation.

Software maintenance

All changes to computer systems are subject to established change management processes and procedures. Software must be actively maintained to ensure that all fixes and patches, needed to avoid significant emerging security risks, are applied as promptly as possible.

High priority patches should either be applied within 5 working days of release or other compensatory control measures taken to mitigate risk.

Systems running software, including the operating system, which are clearly not being maintained adequately and which may be presenting a wider risk to security are liable to have their network connectivity withdrawn.

Software removal

Software that is not licence compliant must be brought into compliance promptly or uninstalled. Software that is known to be causing a serious security problem, which cannot be adequately mitigated, should be removed from service.

When decommissioning a computer system, for disposal or re-use, appropriate measures must be taken in relation to any software stored on it. Software must be removed, where not doing so could lead to breaking the terms of its licence.

8. Mobile and Remote Working

Contents

Introduction

This Mobile and Remote Working Policy sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices which are not located on company premises when these devices are used to access company information assets.

While recognising the benefits to Elliott Training of permitting the use of mobile devices and working away from the office, Elliott Training also needs to consider the unique information security challenges and risks which will necessarily result from adopting these permissive approaches. Elliott Training must ensure that any processing of personal data remains compliant with the Data Protection Act/ GDPR Regulations.

Definition

A mobile computing device is defined to be a portable computing or telecommunications device which can be used to store or process information. Examples include laptops, netbooks, smartphones, tablets, USB sticks, external or removable disc drives, flash/memory cards and wearable devices.

Personally owned devices

Whilst the Elliott Training does not require its staff to use their own personal devices for work purposes, it is recognised that this is often convenient and such use is permitted subject to the following requirements and guidelines.

Users must at all times give due consideration to the risks of using personal devices to access company information and in particular, information classified as confidential.

- The device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- Mobile devices must be encrypted. (Some older devices are not capable of encryption and these should be replaced at the earliest opportunity.)
- An appropriate passcode/password must be set for all accounts which give access to the device.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to “autolock” after a period of inactivity (no more than 10 minutes).

- Devices must remain up to date with security patches both for the device's operating system and its applications.
- Devices which are at risk of malware infection must run anti-virus software.
- All devices must be disposed of securely.
- The loss or theft of a device must be reported to IT Services.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to restricted company information assets.

In addition to the above requirements, the following recommendations will help further reduce risk:

- Consider configuring the device to "auto-wipe" to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (e.g. by "jail breaking" or "rooting" a smartphone).
- Do not leave mobile devices unattended where there is a significant risk of theft.
- Be aware of your surroundings and protect yourself against "shoulder surfing".
- Minimise the amount of restricted data stored on the device and avoid storing any data classified as confidential.
- Access restricted information assets via the companies' remote access facilities (the "remote staff desktop") wherever possible rather than directly.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Reduce the risk of inadvertently breaching the GDPR Regulations by ensuring that all data subject to the Regulations which is stored on the device is removed before taking the device to a country outside of the European Economic Area (or the few other countries deemed to have adequate levels of protection).

Company owned devices

Elliott Training provides computing devices to some of its members. When it does, it will supply devices which are appropriately configured to ensure that they are as effectively managed as devices which remain within the office environment.

Devices supplied by Elliott Training must meet the minimum-security requirements listed above for personally owned devices. In addition, the following are required:

- Non-employees (including family and friends) must not make any use of the supplied devices.
- No unauthorised changes may be made to the supplied devices.
- All devices supplied must be returned to the company when they are no longer required or prior to the recipient leaving the company.

Third party devices

In general, employees should not use third party devices to access restricted company information assets. This includes devices in public libraries, hotels and cyber cafes.

On occasion, employees may be supplied with computing devices by third parties in connection with their work. These devices must be effectively managed, either by the third party or by Elliott Training or by the end user. In all cases, the device must meet the minimum-security requirements listed above for personally owned devices.

Reporting losses

All employees have a duty to report the loss, suspected loss, unauthorised disclosure or suspected unauthorised disclosure of any company information asset to Sarah Elliott.

9. Encryption

Contents

Introduction

This Encryption Policy sets out the principles and expectations of how and when information should be encrypted.

When to use encryption

Encryption must always be used to protect strictly confidential information transmitted over data networks to protect against risks of interception. This includes when accessing network services which require authentication (for example, usernames and passwords) or when otherwise sending or accessing strictly confidential information (for example, in emails).

Where confidential data is stored on or accessed from mobile devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders) the devices themselves must be encrypted (using "full disk" encryption), irrespective of ownership.

Where confidential data is stored in public, cloud based storage facilities the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data.

Where data is subject to an agreement with an external organisation, the data should be handled (stored, transmitted or processed) in accordance with the organisation's specified encryption requirements.

Key management

In most cases, encryption keys will be in the form of a password or passphrase. Losing or forgetting the encryption key will render encrypted information unusable so it is critical that encryption keys are effectively managed. When devices are encrypted by IT Support, IT support will take responsibility for the secure management of the keys. In all other cases, it will be the individual's responsibility to manage the keys. It is advisable to make secure backups of your keys and to consider storing copies with trusted third parties.

Encryption standards

There are many different encryption standards available. Only those which have been subject to substantial public review and which have proven to be effective should be used. Specific guidance is available from IT Support.

UK law

Export regulations relating to cryptography (encryption) are complex, but so long as the encryption software used to encrypt a device or file is considered to be a "mass market" product it is unlikely that you will encounter any problems leaving or re-entering the UK. That said, you may be required to decrypt any devices or files by UK authorities on leaving, entering or re-entering the country. If you are requested to decrypt your files or devices you are advised to do so. Section 49 of the Regulation of Investigatory Powers Act (RIPA) includes a provision whereby certain "public authorities" (including, but not limited to law enforcement agencies) can require the decryption of devices or files. Failure to comply with such a lawful request is a criminal offence in the UK.

Travelling abroad

In addition to what has been written above about export regulations, you should also be aware that government agencies in any country may require you to decrypt your devices or files on entry or exit from the country. If you are travelling abroad with encrypted confidential data this means that there is a risk that the data may have to be disclosed and you should consider the consequences of this. Wherever possible, do not take confidential data with you when you travel (keep the data on Elliott Training servers and access it using the secure remote access facilities). Attention should be paid to the possible inadvertent export of data subject to the Data Protection Act/ GDPR Regulations to countries outside of the EEA (or the few other countries deemed to have adequate levels of protection) when travelling

10. Password Management

Contents

Introduction

This Password Management Policy sets out the requirements for the effective management of passwords and access rights.

Scope

All information systems used to conduct Elliott Training business, or which are connected to the companies network or clients of Elliott Training must be managed in accordance with this policy.

Password management

All passwords should be stored inside the Elliott Training LastPass account in the correct folder appropriate to the account.

Passwords should not be stored outside the Elliott Training LastPass account for any reason.

(IF we end up using LastPass)

LastPass security

All staff accounts must have two factor authentication enabled. Access to the Elliott Training LastPass account is restricted from outside of the UK.

Account and privilege management

Within LastPass staff must ensure passwords are stored in the correct folder to ensure only the relevant staff have access to the passwords needed for their role.