Encryption Policy

Security Incident Reporting Quick Reference

Note! Regardless of confidence level, all security incidents must be immediately reported by phone *and* email. So even if the security incident is only potential or suspected—it must still be reported without delay.

Contact by Mail *and* by Phone	Comment
dataincident@mytutor.co.uk	Use email *and* phone below
07748644728	The Firm Support Number
"The Firm"/ MyTutor	MyTutor

Document Approval

This document has been approved by the following

Role	Name	Version Details
CEO MyTutor	Bertie Hubbard	See section 10.4 Version Control, and section 10 Document Control

Contents

1 Overview

Encryption technologies provide a level of protection for the storage, transmittal, retrieval and access to this data. Encryption works by converting data to make it inaccessible and unreadable to unauthorised individuals. The only way to read the encrypted data is by using a decryption key.

The Data Protection Regulations requires MyTutor to have appropriate policies and procedures in place to ensure the safe keeping, use, retrieval and access to data covered by the Act MyTutor has a responsibility to ensure the integrity, security and protection of all data which it holds.

2 Scope

This policy covers all electronic data and details the types of devices which are acceptable for the storage / transmittal of data, and how these devices utilise encryption software, irrespective of whether or not the data held on them is considered sensitive or confidential. This policy covers encryption for the following devices and applications:

- Desktop, laptop, tablet computers.
- Handheld devices such as mobile phones and PDAs.
- Portable storage devices e.g. USB memory sticks, external drives.
- Removable media e.g. floppy disks, DVD's / CD's, backup tapes.
- Email.

MyTutor's "Internet and E-mail Acceptable Use Policy" provides more general information on the e-mail service and use and is available from MyTutor's intranet or by request to the IT Department's Service Desk.

3 Purpose

The purpose of this policy is to:

- Detail the specification and deployment of data encryption software for the protection of electronic information held by MyTutor.
- Provide guidance on the responsibilities of the use and handling of portable media.
- Provide clarity on the types of portable storage and CTO which are allowed for use.
- Describe how encryption will be used and applied to devices.
- Provide guidance on the responsibilities of the use of encrypted devices.
- Detail the method of reporting breaches of this policy whether intentional or accidental.

4 Policy Statement

4.1 Encryption

1. Full disk encryption will be rolled out gradually to all computers across MyTutor.
The encryption software employed for use at MyTutor uses a minimum of AES 256 bit (Advanced Encryption Standard) which is a symmetric-key encryption with a 256-bit key.

4.2 Objectives

1. Full disk encryption ideally linked to the bios to prevent hard disk swapping will be rolled out to all computers by the IT Department as part of desktop upgrades.

2. MyTutor's data should not be stored on computers or portable media devices unless access is required when network connectivity is not available. When it is necessary data should only be stored on authorised devices.

3. Encryption is applied to all authorised data storage devices attached to desktop, laptop or tablet computers. In certain cases, it may not be feasible for certain devices to be encrypted and each exception to a device will be given full and careful consideration as to its use and any decision made will be based on best practice and MyTutor need.

4. Where exceptions have been identified for not encrypting specific devices, computer policy settings (enforced at domain level) which enable/disable encryption can be applied individually to a specified computer and/or groups of computers.

5. When a portable device, MyTutor's recommended data storage device is used, the instructions for the correct use must be followed to ensure the data is encrypted.

6. Personal storage media and equipment must not be connected to MyTutor's network and must not be used to store MyTutor's data.

7. Other portable USB devices include mobile phones, cameras, PDAs etc. These other devices should not be used to store MyTutor's data. You must contact the IT Department if you need to use these devices as part of your job.

8. If clarification is needed as to the recommended USB data storage devices allowed for use, the IT Department should be contacted.

9. The Security Officer will advise on the best method to encrypt individual files.

4.3 Method

On encryption of an authorised portable storage device (e.g. USB data stick) the user will need to set a password for accessing the device. The password for encrypted portable devices will be in line with MyTutor's password policy and be enforced at the domain level. Using the portable device on any other computer after being encrypted will require a password in order to access it. It is important that local procedures are put in place to ensure that passwords used to encrypt devices are approved by line managers, so that in the event an individual leaves MyTutor, access can be gained to MyTutor's data.

The use of DVD/CD devices and floppy drives will be restricted to read-only access – this will be enforced at the domain level by MyTutor's Policy.

Where there is a need for a particular job function requiring write access to CD/DVD or floppy drives, this can be enabled as an exception and recorded formally with agreement from the IT Department. Any agreement to allow write access of CD/DVD or floppy devices will include the conditional use of appropriate 3rd party archiving (zip) compression/encryption software to be used to encrypt any data stored or written to these devices. This conditional encryption/compression software will be made available as recommended by the IT Department.

Any other requirement for portable storage device such as portable hard drives, magnetic/DAT tapes and devices must be discussed with the IT Department and only hardware and software on MyTutor's approved software and hardware list is to be used.

Computers requiring encryption for the protection of vulnerable and sensitive data will use appropriate encryption prior to subsequent rollout on MyTutor's network.

4.4 Responsibilities

MyTutor has a responsibility to provide its employees with the appropriate secure storage mechanisms, procedures devices and software for the secure handling, storage and retrieval of all electronic data held by MyTutor. The use of portable devices may be subject to random periodic review by MyTutor to ensure compliance with the encryption policy.

All MyTutor's employees, partner agencies, contractors and vendors have a duty to abide by all MyTutor's policies and procedures to ensure the safe, secure handling of all electronic data.

4.5 Use of portable storage media and devices

MyTutor's employees, partner agencies, contractors and vendors undertaking work for MyTutor who are issued with portable storage devices, writing to portable storage media, viewing/transmitting encrypted data or accessing have a responsibility to ensure:

- No one other than authorised person/s are aware of the encryption/decryption password for the device, media or system.
- Any portable device or media is not given to any unauthorised persons for safe keeping.
- Any portable device or media is not left discarded or unattended in a public place.
- All reasonable steps are taken to ensure that during transit, any portable device/media is locked via a key or combination lock and securely located. Portable devices/media must not be left unattended in any vehicle at any time due to insurance requirements.
- Any portable device or media is adequately protected from physical damage.
- Any portable device or media is not hired, lent out or given without authorisation from the IT Department.
- Any portable device or media which is no longer required or has reached its lifespan must be handed over to the IT Department. All data on the device/media must be wiped, destroyed and disposed of through MyTutor's ICT disposal procedure.
- The device/media is handed back to the IT Department on cessation of employment with MyTutor.
- The device/media is handed back to the IT Department when no longer authorised to use the device/media.
- The loss of any portable device is notified immediately via MyTutor's Incident Escalation procedure on the front page of every document.

5 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to MyTutor assets, or an event which is in breach of MyTutor's security procedures and policies.

All employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through MyTutor's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of MyTutor.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of MyTutor's ICT systems or network results from the non-compliance, MyTutor will consider legal action against the third party. MyTutor will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under MyTutor’s disciplinary process.

6 Definitions

Term	Description
Information	Any information, data or record irrespective of format, collected, generated or used by a MyTutor system or process. Examples include electronic communications, emails, digital recordings such as Call Centre Telephone conversations and CCTV, hard copy (paper) files, photographs, maps, plans, process documentation (code, scripts, etc.) and technical drawings.
Information Classification	Assigning a piece of information to a particular category based on its content
Information [Asset] Owners	Executive and Senior managers who are responsible for managing the acquisition, creation, maintenance, usage and disposal of MyTutor’s Information and Information Systems within their assigned area of control
Information Risk	That part of MyTutor’s overall risk portfolio which relate to the confidentiality, integrity and availability of information within MyTutor.
Information Security	The ability to protect the confidentiality, integrity and availability of information held by MyTutor, including any sub-contractors and suppliers, from unauthorised use, disclosure, modification, damage or destruction be it accidental or malicious.
Information Security Breach	An Information Security Incident where it is confirmed that a stated organisation policy or legal requirement regarding Information Security has been contravened.
Information Security Incident	Any event/information that warrants concern by MyTutor Information Security that may also possibly affect MyTutor Customer information systems, clients, or MyTutor partners.
Information System	Information in any media type, hardware, software, supporting networks, processes and human resources that support its acquisition, processing, storage and communication.
Secure	A term used in this document to define the requirement to manage information in a manner so as to minimise the risk of a Security Incident occurring through unauthorised disclosure or access to controlled information
The Firm	MyTutor classified as Private Limited Firm
MyTutor Personnel	Includes all MyTutor employees as well as all temporary staff, contractors, consultants and any third party with whom special arrangements have been made e.g. Confidentiality and Non-Disclosure Agreements.
CTO	Chief Technology Officer
Security Forum	MyTutor forum where information security matters are discussed and activities related to information security are co-ordinated.
CIRO	Chief Information Risk Officer

Term	Description
ICT	ICT, or information and communications technology

7 Duties and Responsibilities for Information Security

Role or Team	Description
Chief Executive Officer	Has overall accountability and responsibility for Information Security within MyTutor on a day-to-day basis the Information Security Lead will be the CEO as the Senior Information Risk Owner.
Senior Information Risk Owner (SIRO)/CTO	Will act as the advocate for information risk on MyTutor Board and in internal discussions, and will provide written advice to the Chief Executive on the content of their annual statement in regard to Information Risk.
Human Resources	Shall be responsible for ensuring that suitable contracts and non-disclosure agreements are in place with external contractors before access to MyTutor Information is given. These contracts require the contractor to comply with all appropriate security policies.
IT Systems and Data Manager	Is responsible for the implementation and enforcement of the Information Security Policy.
Line Managers	Are responsible for ensuring that all their staff (permanent and temporary) and contractors are aware of the Information Security Policy and that it is implemented fully in their area of responsibility.
Procurement	Shall be responsible for ensuring that suitable contracts with non-disclosure clauses are in place before access to MyTutor Information is given. These contracts shall ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.
Security Forum	Is responsible for ensuring that MyTutor complies with the Data Protection Act 2018 and as amended and that Information Governance standards are effectively managed and implemented.

8 Policy Review

This policy will provide a measure against which information security incidents can be assessed and subsequently managed.

MyTutor (via the Security Forum) will review this policy on an annual basis or in response to an actual or perceived increase in information security risk.

9 References

These references below are those most directly relevant.

#	Title	Description	Comment
Error! Bookmark not defined.			This is likely to be updated so always check for the latest version
1			
2			
3			This is likely to be updated so always check for the latest version
4			
5	The Regulation Register	Current list of legislation relevant to MyTutor	This is likely to be updated so always check for the latest version

10 Document Control

10.1 Contributors, Reviewers, and Approvers

#	Role	Name	Comment
1	Approver—MyTutor	Bertie Hubbard CEO	
2	Content Author		
3	Reviewer	Michael Nuttall CTO	
4	Producer		

10.2 Document Maintenance

This section holds central information, it includes ‘bookmarked’ data which can then be reflected into other parts of the document.

#	Name	Variable	Description	Comment
1	Next Review Date	22/7/2021	The latest date by which this document needs to be reviewed	This document is intended to be reviewed annually by the Security Forum. It can be

#	Name	Variable	Description	Comment
				reviewed prior to date here. This will be set when the document is Released
2	Document Date	04Sep2020 08:39	The date for this version of the document. It uses the `DM_Document_Date` bookmark	For Approved versions this will usually use the {SAVEDATE} field code. Released versions will use a text string for the date
3	Expiry Date	ddMMMyyyy	Date at which the document is marked for deletion	This would only be applied if decided at review.
4	Status			Currently uses DOCPROPERTY `Status` Custom field
5	Version Number			Currently uses DOCPROPERTY `Version` Custom field

10.3 Document Access Control Categories

The access categories/classifications in use

#	Category (Classification)	Circulation	Comment
1	MyTutor Internal	Can only be circulated to MyTutor personnel, and selected approved MyTutor partners/third party suppliers	
2	MyTutor Edit	“MyTutor”	The list for Read/write/edit is provisional and can be extended

10.4 Version Control

Version	Status	Actions	Action By	Date Started
0.1	Draft	Initial draft: replaced all previous information security polices		
1.0	Released	Reviewed and Amended for Final Release		

Version	Status	Actions	Action By	Date Started
1.1	Released	Minor amendments		

10.5 Applied ISO27001 Controls

Control Ref	Title
A.6.2.1	Mobile device policy
A.8.2.1	Classification of information
A.8.2.2	Labelling of information
A.8.1.4	Return of assets
A.14.2.7	Outsourced development
A.15.1.1	Information security policy for supplier relationships
A.15.1.2	Addressing security within supplier agreements
A.15.1.3	Information and communication technology supply chain
A.15.2.1	Monitoring and review of supplier services
A.15.2.2	Managing changes to supplier services