Laptop & Mobile Device Security Procedure

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

MyTutor recognises that laptops, tablets, PDAs and other mobile computing devices are useful tools which enable more convenient, flexible mobile working across MyTutor network however; mobile computing devices must be controlled, configured and used in the most secure way possible using standards and procedures to prevent damage to assets and reputation of MyTutor.

2 Scope

This scope of this policy extends to all departments, employees, contractors, vendors and partner agencies who utilise or who are responsible for the development, management/maintenance of information within MyTutor's ICT processing facilities.

3 Purpose

The purpose of this procedure is to ensure that laptops, tablets and other mobile computing devices are used, configured and managed in a secure and safe way and to identify and describe the steps required to achieve and maintain this

4 Policy Statement

4.1 Laptop and Tablet Devices

All laptop and tablet computers owned by MyTutor are supplied to users with a preconfigured standard Windows Operating System image which the IT Service has developed and approved. This preconfigured image may vary slightly due to differing departmental requirements and needs, however, in terms of security; all laptop and tablet devices connected to MyTutor's network domain will all have the same level of security applied across all areas.

All MyTutor's laptops/tablets are subject to the following configuration which ensures they are added to MyTutor's network and have the correct security configuration settings applied:

Currently, new laptops/tablets arriving at MyTutor will already have the approved "standard" build applied. The configuration of the laptop/tablet image involves the installation of additional software (which will vary between departments) and some changes which may be necessary for optimisation of the operating system.

Currently, newly commissioned laptops/tablets are added to MyTutor Domain using an asset tag number as required or Identifier.

N.B. It is planned that these prefixes will not be necessary and may be dropped in the future.

Laptops/tablets can only be added to the Domain and configured with a computer account, by IT Service staff that are authorised and have sufficient access permissions to do so. Authorised staff are required to logon “locally” to the laptop/tablet using the built-in Administrator’s account in order to add the laptop/tablet to the Domain. During the process of adding the computer to the Domain, authorised staff are required to provide a valid MyTutor account username and password to complete the process.

Laptops/tablets which have not been added to MyTutor’s network Domain are not able to participate in MyTutor’s network and will not be able to authenticate and service user logons – irrespective of the level of access the user may have with their Domain account while attempting to logon.

Laptops/tablets are protected from viruses and spyware/malware using MyTutor’s Build standard, an industry standard antivirus/malware software product which is automatically installed on all laptops/tablets during boot up and is regularly updated with the latest virus/malware definition files.

Laptops/tablets which are for use in partner agency areas are subject to the same security restrictions enforced by MyTutor’s network domain. Any network accounts used to access these laptops/tablets are managed and authorised by the IT Service.

N.B. Laptops/tablets which have not been provided by MyTutor but have been approved for use will be subject to the relevant security checks and procedures by the IT Service.

As standard "auto-run" or "auto-play" is disabled on all systems.

4.2 Other Mobile Computing Devices

The software in use across MyTutor, both legacy and newer systems have been evaluated, purchased and installed on the basis of minimum specification requirements which, for the most part, involves running software which is supported by the vendors/contractors.

Other mobile computing devices which do not satisfy the hardware and/or minimum software (Operating System) installation specification should not be used to run MyTutor applications nor should any attempts be made to use or bypass application/system authentication processes or controls when using such devices.

Other mobile computing devices (i.e. not a laptop or tablet) used for MyTutor's business should primarily be used as a "resource" tool – providing and acting as an enabler to access information from MyTutor's website, intranet and other web-based information and resource sites.

Connecting any mobile computing device to MyTutor's network must be evaluated by the IT Service and subject to existing configuration standards and procedures of MyTutor. The IT Service must be contacted for the approval or configuration of any of these devices whether the connection is to be made wirelessly or wired.

4.3 Use

MyTutor's laptops, tablets and other mobile computing devices may only be used by authorised parties for authorised MyTutor business or purposes in accordance with MyTutor's Acceptable Use Policy and associated security policies. MyTutor's employees, partner agencies, contractors and vendors must be mindful of the potential for unauthorised access and viewing of MyTutor's data and Information and take appropriate steps to avoid or prevent this.

All users of MyTutor's laptop, tablet and other mobile computing devices must ensure at all times that:

Account logon and system passwords are kept private and not shared, displayed or communicated to anyone else.

Sensitive and personal data must not be saved on any mobile computing device under any circumstances.

Data which is not sensitive or person identifiable may be stored to mobile computing devices only when MyTutor Corporate network is unavailable - data should then be transferred to the Corporate network once it becomes available again and local copies of data should be deleted.

Users must be made aware that data stored locally on CTO will not be backed up and is at risk from being lost.

Mobile computing devices must not be treated as data storage devices – only portable media which has been encrypted and agreed for use in accordance with MyTutor's Encryption Policy may be used to store MyTutor's data.

Data and Information which is accessed or saved to portable storage devices (e.g. USB data stick - not on the mobile computing device itself) via a laptop, tablet or other mobile computing device must only be copied to a storage device which is encrypted in accordance with MyTutor's Encryption Policy.

Screens on mobile computing devices must be locked by users when away from the device or if left unattended.

Unauthorised, non-standard or personal equipment must not be plugged-in or inserted into the mobile computing device.

Software must not be installed on the laptop, tablet or mobile device by unauthorised staff.

Any software installed must be (or going through the process of being) placed on the approved software list.

Mobile computing devices must not be mishandled, wilfully damaged or tampered with in any way – this includes taking off the device case cover (other than for the replacement of batteries or extended memory card/s) or removing of any screws or fixings.

Mobile computing devices are logged off and shut down when not in use for extended periods and are powered off.

Any mobile computing device is not given to any unauthorised persons for safe keeping.

Any mobile computing device is not left discarded or unattended in a public place.

All reasonable steps are taken to ensure that during transit, any mobile computing device is locked via a key or combination lock and securely located. Portable mobile computing devices must not be left unattended in any vehicle at any time due to insurance requirements.

Any mobile computing device must be adequately protected from physical damage.

Any mobile computing device is not hired, lent out or given without authorisation from the IT Service.

Any mobile computing device which is no longer required or has reached the end of its useful life must be returned via the line manager to the IT Department to be disposed of through MyTutor's ICT disposal procedure.

All mobile computing devices must be handed back to the IT Department via the line manager on cessation of employment with MyTutor or when no longer required as part of an individual's current employment.

All CTO must be made available when requested by the IT Service/authorised officers for maintenance and policy compliance reviews.

Care is taken when using remote connections including wireless network points that these are "trusted" and adequately secured – further guidance is available in the Wireless Access Policy.

N.B. Loss of any mobile computing device must be reported immediately to the IT Service, Service Desk

4.4 Maintenance

All maintenance of mobile computing devices is carried out by IT Service authorised staff.

Only staff working within an ICT function (or persons authorised by the IT Service) may perform maintenance, install applications/software or make system configuration changes to mobile computing devices. Staff may occasionally be requested to assist while under the supervision and authorisation of the IT Service as appropriate.

A standard base configuration is installed on all MyTutor's laptop and tablet devices. Any variations and additions must be agreed by the IT Service and the Security/Business Continuity Manager must be notified.

Laptops/tablets are protected against malicious code in accordance with MyTutor's malicious software and anti-virus Procedure.

All mobile computing devices are maintained in accordance with all relevant policies and procedures of MyTutor.

All operating system software and firmware must be receiving regular security updates from the supplier.

Windows and Mac devices are set to update automatically.

4.5 Disposal

All mobile computing devices which are scheduled for replacement will be disposed of by the IT Service through MyTutor's ICT disposal procedures.

Without exception, any computer or device which is used for the handling or creation of MyTutor's data must be secured and is subject to all the relevant policies and procedures specific to the security of ICT equipment and its use.

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
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 MyTutorBoard 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
1			This is likely to be updated so always check for the latest version
2			
3			
4			This is likely to be updated so always check for the latest version
5			
6	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 reviewed prior to date here. This will be set when the

#	Name	Variable	Description	Comment
				document is Released
2	Document Date	04Sep2020 08:41	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	ddMMyyyy	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		
1.1	Released	Minor amendments		
1.2	Released	Minor amendments		

Version	Status	Actions	Action By	Date Started

10.5 Applied ISO27001 Controls

Control Ref	Title
A.6.2.1	Mobile device policy
A.8.1.3	Acceptable use of assets
A.8.2.3	Handling of assets
A.8.3.1	Management of removable media
A.8.3.2	Disposal of media
A.9.4.4	Use of privileged utility programs
A.9.4.5	Access control to program source code
A.11.2.1	Equipment siting and protection
A.11.2.4	Equipment maintenance
A.11.2.6	Security of equipment and assets off-premises
A.11.2.7	Security disposal or re-use of equipment
A.11.2.8	Unattended user equipment
A.12.5.1	Installation of software on operational systems
A.16.1.2	Reporting information security events