Teleworking and Mobile Working Procedures

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 Business Support Number
"The Business"/ MyTutor	

Document Approval

This document has been approved by the following

Role	Name	Version Details
CEO MyTutor	Bertie Hubbard	See section 11.4 Version Control, and section 11 Document Control

Contents

1 Overview 3
2 Scope 3
3 Purpose 4
4 Responsibilities 4
5 Procedure Statement 4
5.1 Wi-Fi Security 7
6 Breaches of Policy 8
7 Definitions 8
8 Duties and Responsibilities for Information Security 9
9 Policy Review 10
10 References 10
11 Document Control 11
11.1 Contributors, Reviewers, and Approvers 11
11.2 Document Maintenance 11
11.3 Document Access Control Categories 12
11.4 Version Control 12
11.5 Applied ISO27001 Controls 12

1 Overview

Teleworking and mobile working is use of Information Communication Technology enabling work on, or access to MyTutor's information, perhaps from locations other than a user's nominated place of work.

Teleworking is defined as working from a fixed remote location, such as home or a touchdown centre. Mobile (remote) working is defined as working in a place that is not an individual's normal work base, which could be a touchdown centre, MyTutor providing guest Wi-Fi hotspots, hotels, airports, conferences – anywhere a connection to a public communications network makes access via secure portals to MyTutor's resources possible.

Webmail is a method of accessing MyTutor's email from a PC or mobile device which has access to the internet via a secure, encrypted web browser session.

This should be used only with Multi Factor authentication or CASB Cloud Access Security Broker system if available.

Working from home, whilst travelling, at a client's site or at any other location away from the established (physical) office may be attractive and offer benefits. However, opening up MyTutor's information and systems through Teleworking/mobile working also presents security risks. Intruders (hackers, electronic eavesdroppers, shoulder surfers, etc.) may be able to access, read and potentially modify MyTutor's information and systems without having to be on site. **A Secure VPN should be used.**

2 Scope

The scope of these procedures includes all persons/parties who have access to information and ICT systems belonging to or under the control of MyTutor; including:

- MyTutor's employees
- Contractors
- Temporary staff
- Partner organisations
- Any other party utilising MyTutor's ICT resources

The following four types of flexible worker profiles are included within the scope: flexible worker, mobile worker, field worker and fixed home worker.

Processing devices that can be used as part of teleworking or mobile working include:- PC's (Home based, touchdown centres etc.), laptops and notebooks, tablet PC's, smart phones, personal digital assistants (PDAs), digital cameras, mobile phones and any other mobile device that record and/or process information.

Removable media is anything that data can be copied, saved and/or written on to which can then be taken away and restored onto another computer (e.g. CD, DVD, flash drives, USB data sticks, portable hard drives.)

3 Purpose

The purpose of these procedures are to ensure that security of information and systems, accessed through teleworking and mobile working are given due importance. It is essential that staff have the knowledge that security procedures and policies exist and they are understood and adhered to.

Information that is related to and can identify an individual is personal data and protected by the principles of the Data Protection Regulations. As such, appropriate technical and organisational measures shall be taken against accidental or deliberate loss, change, destruction of, or damage to personal data. These procedures have been produced to ensure that protection of personal data is maintained whilst remote working.

4 Responsibilities

Directors are responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure all staff has sufficient, relevant knowledge concerning the security of information and systems. Designated owners of systems, who have responsibility for the management of ICT systems and information, need to ensure that all staff is aware of their responsibilities towards security. Designated owners of systems and information need to ensure they uphold the security policies and procedures.

Users must have read the rules, regulations and guidelines which advise the correct methodology for using Webmail prior to trying to access their MyTutor email using this system.

5 Procedure Statement

Access to Office 365 and G suite must follow the latest NCSC guidelines

1. For teleworking and mobile working, access to MyTutor's information, networks and applications (Including MyTutor's email) can be attained via the secure (Virtual Private Network) access portal of MyTutor. This requires two factors of authentication, a computer based certificate and User ID/Password. MyTutor's CTO that have been used to log directly on to MyTutor network at the workplace will have the computer based certificate.

2. Desk and successful approval from the IT Director, certificates can be installed.

3. It is possible to access MyTutor's email from a remote location (Such as home) using non-wireless or wireless technology.

Staff must ensure when using this service that https is displayed at the start of the address line and the padlock symbol is displayed on the browser window. At the end of using this email service staff must logoff MyTutor's webmail and close the browser window. Failure to do so can leave the account accessible to hackers.

4. Connection to MyTutor's network should only be attempted using the domain logon and password credentials that staff are issued with. Connection using network infrastructure that does not belong to MyTutor may enable traffic to be viewed, altered or deleted by an attacker.

5. Extra care should be taken to properly close all applications, network connections and web browsers when using PC's, CTO and software not officially provided by MyTutor. Passwords, logon credentials and sensitive files can be left behind on un-trusted devices, making them readily available to subsequent users.

6. All users accessing MyTutor's networks or specialised external services via teleworking and CTO must abide by associated security policies of MyTutor and any applicable codes of connection and conduct.

7. Managers are responsible for ensuring that their staff knows how to use approved devices and software to connect to and safely/securely use MyTutor's networks via teleworking/mobile working.

8. Managers of staff for whom they have responsibility must ensure they have up to date contact and device information for their staff making use of teleworking / mobile working.

9. Users conducting teleworking/mobile working should not allow or give permission for unauthorised users (including family and friends) to use that PC/mobile device.

10. Any information concerning passwords, usernames, network credentials or requirements/ability used to access MyTutor's information and systems by teleworking/mobile working must not be shared with other staff, unauthorised users, third party vendors, family, friends or members of the public.

11. Teleworking and/or CTO distributed by MyTutor should only be used by authorised parties for authorised MyTutor business or purposes in accordance with MyTutor's Acceptable Use Policy and associated security policies.

12. Adherence to MyTutor's Acceptable Use Policy and security policies is a requirement of teleworking and mobile working.

13. Users should always be aware of the potential for other people (including family, friends, colleagues and intruders) to overlook screens and keyboards and view personal, confidential information or passwords. Users should check this is not taking place.

14. During short periods of time when devices are not being used (e.g. when on the phone) users should lock PC's and devices to prevent screens being overlooked. For example, on PC's/laptops this can normally be achieved by holding down the ctrl-alt-del keys together and choosing the 'lock computer' option or by holding down the Windows (flag) key and hitting the L key.

15. Users should ensure that all applications are properly closed / logged off, browsers are closed and internet sessions are logged off, prior to network connections being logged off and closed.

16. On completion of work, teleworkers/mobile workers should fully power down or log off remote devices. Devices should not just be suspended.

17. Active equipment that is unlocked and in use should not be left unattended at any time.

18. A password should be set up and used on all equipment that can be locked by use of a password. For example iPAQ devices can be set locked using a password and this facility should not be disabled by the user.

19. Transfer of personal or restricted information must take place through a secure, encrypted channel (identified by the https address prefix and padlock symbol) using suitable software/applications.

20. Person identifiable information and/or business data should not be stored on the PC/mobile device. If possible data should be accessed from and be stored on MyTutor's servers or on password protected and encrypted portable / removable media.

21. Users must not install or update any software on owned or managed devices by MyTutor.

22. Users must not install any screen savers on owned or managed devices by MyTutor.

23. Users must not download or install any applications or items on owned or managed devices by MyTutor from the internet unless official authorisation has been gained from the IT Department.

24. Users must not alter or disable any element of the configuration of devices, including data encryption and anti-virus software.
25. Only MyTutor provided removable media should be used and must be safely 'closed' if necessary and removed from any device when finished with.

26. Person identifiable information and data should only be sent using official channels, authorised software/applications and official equipment deemed fit for the purpose. For example, text messages containing person identifiable information and data should not be sent via mobile phone.

27. Staff entrusted with MyTutor's CTO are responsible for ensuring that it is regularly connected to MyTutor network for automatic upgrade of anti-virus software and other software licensing agreements.

28. If it is likely that a device will not be connected to MyTutor's network for a period of greater than 14 days, then that device should be entrusted with a line manager for connection to the network for anti-virus and software licensing upgrade requirements.

29. In the event that a user becomes aware of an information or data breach or accidental disclosure, this matter must be reported immediately via MyTutor's Incident Reporting Procedures.

5.1 5.1 Wi-Fi Security

Computers and many other devices, including smart phones and PDAs, can connect to the internet wirelessly using Wi-Fi. An unsecured Wi-Fi connection makes it easier for hackers to access private files and information and it allows strangers to use the internet connection for their own purposes. These are general tips on changing private router and network settings. Staff may need to check the instructions for their wireless equipment for the technical details. If staff need more guidance on checking or changing settings, the Wi-Fi equipment supplier or internet provider will provide advice on their websites.

How do I check whether my network is secure?

Wi-Fi networks are accessed through a physical device called a router – also known as a hub. Staff will need to connect to their router to check its network settings. To do this, staff will need the router's IP address, user name and password. Open the browser and enter the router's IP address into the address bar. When asked, enter username and password. The router settings will allow staff to find out whether the connection is already secured and will let a more secure password be chosen.

How do I secure my network?

The following tips will help staff to use Wi-Fi more securely and to protect personal information.

Change the wireless network's default name

A Service Set Identifier (SSID) is a unique ID used for naming wireless networks and ensures the network name is different to other nearby networks. Staff should change the network name from the router's default. This will make it harder for anyone to identify the browser and guess its default settings.

Use encryption

Encryption scrambles messages sent over wireless networks so that they cannot be read easily. If the network is not encrypted then staff should enable encryption on their settings page. There are different forms of encryption, but MyTutor requires that staff use the Wi-Fi Protected Access (WPA/WPA2) version because it is stronger than other versions such as Wired Equivalent Privacy (WEP) (MyTutor states staff must use WPA2.)

Choose a strong password

Change the password from a default supplied with the router. Make sure the password is easy to remember but would be difficult for a stranger to guess and preferably something with a combination of letters and numbers. Avoid using something obvious such as street name (MyTutor requires staff to follow its Password Policy.)

Hide the network ID

A router broadcasts its SSID to anyone within range. When the option is available staff should alter the router settings to not broadcast the SSID and therefore avoid alerting hackers to the network's existence.

Check that the device does not auto-connect to Wi-Fi signals

If the device is set to automatically connect to available Wi-Fi networks then staff run the risk of automatically connecting to unknown and potentially dangerous networks. Staff should switch off auto-connect on the device settings page – refer to the manufacturer's instructions for more details.
.

6 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.

7 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

Term	Description
Information [Asset] Owners	Executive and Senior managers who are responsible[1] 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[2]
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.
CEO	Chief Information Risk Officer
ICT	ICT, or information and communications technology

8 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	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

Role or Team	Description
(SIRO)/CTO	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 Working Group (SWG)	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.

9 Policy Review

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

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

10 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

11 Document Control

11.1 Contributors, Reviewers, and Approvers

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

11.2 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 SWG. It can be reviewed prior to date here. This will be set when the document is Released
2	Document Date	04Sep2020 08:40	The date for this version of the document. It uses the `DM_Document_Date` bookmark	For draft 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

11.3 Document Access Control Categories

The access categories/classifications in use

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

11.4 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		

11.5 Applied ISO27001 Controls

Control Ref	Title
A.6.2.1	Mobile device policy
A.6.2.2	Teleworking
A.8.3.2	Disposal of media
A.8.2.3	Handling of assets
A.9.3.1	Use of secret authentication information
A.11.1.5	Working in secure areas
A.11.2.1	Equipment siting and protection
A.11.2.6	Security of equipment and assets off-premises
A.11.2.8	Unattended user equipment
A.13.2.1	Information transfer policies and procedures