Security Incident Management 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 9.4 Version Control, and section 9 Document Control

Contents

1 Overview

MyTutor is responsible for the security and integrity of all data it holds. MyTutor must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to MyTutor's assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security:

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
- Loss of confidentiality of information
- Compromise of integrity of information
- Denial of service
- Unauthorized access to systems
- Misuse of systems or information
- Theft and damage to systems
- Virus attacks
- Intrusion by humans

Other incidents include:

- Loss of ID badge/s
- Missing correspondence
- Exposure of Uncollected print-outs
- Misplaced or missing media
- Inadvertently relaying passwords

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent incidents occurring.

More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

2 Scope

The scope of this policy extends to all departments, employees, contractors, vendors and partner agencies who use/access MyTutor's ICT facilities.

- This policy applies to:
- All of MyTutor's departments, personnel and systems (including software) dealing with the storing, retrieval and accessing of data.

3 Purpose

The purpose of this Acceptable Policy is to apply acceptable use controls to Information, Information Systems, software Applications, Communication Networks, and CTO, used throughout.

4 Policy Statement

MyTutor has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing MyTutor's employees, partner agencies, contractors and vendors of the importance of the identification, reporting and action required addressing incidents; MyTutor can continue to be pro-active in addressing these incidents as and when they occur.

All MyTutor employees, partner agencies, contractors and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via MyTutor's Incident Reporting procedures.

The types of Incidents which this policy addresses include but is not limited to:

4.1 Computers left unlocked when unattended

Users of MyTutor's computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All MyTutor's employees, partner agencies, contractors and vendors need to ensure they lock their computers appropriately - this must be done despite the fact that MyTutor computers are configured to automatically lock after 5 minutes of idle time.

Discovery of an unlocked computer which is unattended must be reported via MyTutor's Incident Reporting procedures.

4.2 Password disclosures

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedures for authorisation – initially through the individual's line manager. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the IT Service must be notified through MyTutor's Incident Reporting procedures. For more information, MyTutor's Password policy is available on the intranet or via the IT Department's Service Desk.

Under no circumstances should an employee allow another employee to use their user account details after they have logged onto a system – even under supervision.

4.3 Virus warnings/alerts

All Desktop, laptop and tablet computers in use across MyTutor have Antivirus (including Anti-Spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to MyTutor's data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported by the user to the IT Department as soon as possible.

4.4 Media loss

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PC's, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any authorised user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental of any portable media must report it immediately through MyTutor's Incident Reporting procedures.

4.5 ID Badges

It is essential for us to identify individuals and wearing ID badges wear necessary helps us to do this.

4.6 Data loss/disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional

- Published on MyTutor's website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function Devices (MFD's)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All of MyTutor's employees, partner agencies, contractors and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of MyTutor's data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using MyTutor's Incident Reporting procedures

4.7 Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc. must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person identifiable information must be reported through MyTutor's Incident Reporting procedures.

4.8 Physical Security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower floor/level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the IT Service via MyTutor's Incident Reporting procedures.

Continuing emphasis and re-enforcement of MyTutor's Secure Desk policy will further help to reduce the number of security incidents.

4.9 Logical Security / Access Controls

Controlling, managing and restricting access to MyTutor's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

4.10 Missing correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no printed output retrieved etc. must be reported through MyTutor's Incident Reporting procedures.

4.11 Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported through MyTutor's Incident Reporting procedures.

4.12 Loss or theft of IT/information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc., or which is known/or suspected to have been stolen needs to be reported immediately through MyTutor's Incident Reporting procedures.

5 Definitions

Term	Description
Information	Any information, data or record irrespective of format, collected, generated or used by a business 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 Business Information Security that may also possibly affect Business Customer information systems, clients, or business 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 Business	MyTutor classified as Private Limited Business
The Business Personnel	Includes all MyTutor's 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's forum where information security matters are discussed and activities related to information security are co-ordinated.
ICT	ICT, or information and communications technology

6 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 the Business 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's 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.

7 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.

8 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

9 Document Control

9.1 Contributors, Reviewers, and Approvers

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

9.2 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 document is

#	Name	Variable	Description	Comment
				Released
2	Document Date	04Sep2020 08:37	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

9.3 Document Access Control Categories

The access categories/classifications in use

#	Category (Classification)	Circulation	Comment
1	CONTROLLED	Can only be circulated to The Business 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

9.4 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		

Version	Status	Actions	Action By	Date Started

9.5 Applied ISO27001 Controls

Control Ref	Title
A.16	Information Security Incident Management