Access Control 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 11.4 Version Control, and section 11 Document Control

Contents

1 Overview 3

2 Scope 3

3 Purpose 3

4 Policy Statement 3

4.1 Systems/Information Access 4

4.2 Systems/Information Deregistration 4

4.3 Logon Considerations 5

4.4 Physical Access and Controls 5

5 Responsibilities 7

6 Breaches of Policy 7

7 Definitions 7

8 Duties and Responsibilities for Information Security 8

9 Policy Review 9

10 References 9

11 Document Control 10

11.1 Contributors, Reviewers, and Approvers 10

11.2 Document Maintenance 10

11.3 Document Access Control Categories 11

11.4 Version Control 11

11.5 Applied ISO27001 Controls 11

1 Overview

Availability, confidentiality and integrity are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital for the protection of systems and information authorised users who have access to MyTutor's systems and information are aware of and understand how their actions may affect security.

Availability – systems and information are physically secure and will be accessible to authorised persons when required.

Confidentiality – systems and information will only be accessible to authorised persons.

Integrity – the accuracy and completeness of systems and information are safeguarded.

Authorised users referred to in this document are members of the following groups:-

All parties (Either as part of a contract of employment or third party contract) who have access to, or use of ICT systems and information belonging to, or under the control of MyTutor including:

- MyTutor employees
- Contractors
- Full and part-time staff
- Temporary staff
- Agency staff
- Partner organisations
- Any other party utilising MyTutor's ICT resources

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 policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

4 Policy Statement

On-going education featuring corporate induction programmes, eLearning, line manager training, specific training and awareness programmes must be undertaken by staff to enable them to be aware of their responsibilities towards systems and information security.

4.1 Systems/Information Access

The Access Control matrix system is for managers to complete if an employee's role within the organisation changes and access to systems needs to be updated or removed. Managers must contact MyTutor system owners to ensure access to other systems and programs are updated if a user's role or business needs change.

- For systems containing restricted and personal information and data, an access control matrix must be developed to record role based authorised access recorded on an individual basis. Authorisation procedures must be in place for managers to authorise all access (including short term and temporary access) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access.
- To gain access to specific systems and information, a member of staff will need to follow a formal application process. Users will need to apply to the relevant owners/senior custodian of the systems using the appropriate completed forms.
- Generic logons are not generally permitted across MyTutor however, use of generic accounts under exceptional 'controlled' circumstances is permitted, and for members of the Dev/Ops team.
- To ensure relevant MyTutor or national legislation security standards are adhered to, personnel checks, such as DBS and Baseline Personnel Security Standard checks may be undertaken if required.
- The appropriate level of access to systems and information will be determined upon the prospective users required business need, job function and role.
- A signed confirmation by the user may be required indicating that they understand and appreciate the conditions of access and security.
- If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the applicant. Further instruction on how to maintain the security of systems and information with due regard to the procedures below may be given.
- Access for remote users shall be subject to authorisation by line managers via the IT Department. No uncontrolled external access shall be permitted to any network device or networked system.
- The application and all other documentation should be maintained in line with all relevant guidance.
- Where staff members use their own personal devices, which require them to enter their personal credentials. All company devices require unique credentials
- A list of all administrative and user accounts within the organisation is aligned with the information asset register and regularly reviewed for privilege needs and requirements.
- Where 2FA is built-in natively and does not require any additional software or hardware it should be used.

4.2 Systems/Information Deregistration

- If a member of staff changes role or their contract is terminated, their manager should apply to have the users access to the system/information reviewed or removed as soon as possible.
- If a member of staff is deemed to have contravened any of the Information Security policies or procedures, potentially jeopardising the availability, confidentiality or integrity of any systems or information, their access rights to the system/information should be reviewed by the system owners.
- If a specific access limit is exceeded or control circumvented several times by a user the manager should review the access rights of the user and if necessary remind the user of the relevant access and security.
- If a number of unsuccessful log-on attempts are exceeded, the user will be informed that they need to contact the system owners or the IT Department to ask for access rights to be re-established. In these circumstances, access rights may need to be reviewed.
- If it is deemed that it is no longer appropriate or necessary for a user to have access to systems and/or information then the user's manager will need to inform the owners of the system/information that access rights should be altered/removed immediately.
- If any system/information rights are altered or removed, the relevant documentation will need to be updated accordingly.
- All user accounts on systems are reviewed and checked if they are needed at least quarterly .
- As part of deregistration the procedure is to delete all accounts associated with that employee.

4.3 Logon Considerations

- All systems should be accessed by secure authentication of user validation. As a minimum this should entail use of a User name and a Password.
- Logon to systems/information should only be attempted using authorised and correctly configured equipment in accordance with MyTutor's policies.
- After successful logon users should ensure that equipment is not left unattended and active sessions are terminated or locked as necessary. Systems should be logged off, closed down or terminated as soon as possible.
- System logon data should not be copied, shared or written down.

4.4 Physical Access and Controls

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data:

- Staff, as needed, wears their MyTutor's ID badges and visitors must wear the Visitor ID badges which have been issued to them. People who are not displaying ID badges should be challenged. Any person not known to location personnel must be challenged in order to establish who they are and whether authorisation has been provided for them to be there. If

there is any doubt about the identity of the individual, the appropriate security officer/manager should be contacted to confirm the individual's identity.

- Appropriate recording mechanisms need to be in place to record the names, dates, times and signatures for the signing in and out of visitors (including MyTutor personnel) to MyTutor's locations. All visitors must be issued with an authorised MyTutor visitors badge when signing in.
- The use of keys to buildings, rooms, secure cabinets, safes etc. must be controlled and recorded. Keys must be stored in secure areas/locked cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be known at all times and a signing in/out recording mechanism must be maintained to record the serial/ID of keys against individual names when keys are used.
- Electronic access fobs must be issued to authorised staff on an individual basis. Staff issued with access fobs must have their names and employee numbers recorded against the registered access fob number including date and time of issue.
- Access fobs should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's fob if available with permission of the line manager and the recorded user must either be present or be made aware that their fob is being used. Any such use must be recorded and maintained in a logging system for this type of event.
- Access fobs issued to personnel who no longer work for MyTutor must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system.
- Locations housing critical or sensitive information and/or information processing facilities should have a secure, physically sound perimeter with suitable controls and restrictions allowing access to authorised staff only. CCTV and audible alarm systems should be active in areas where critical servers are located, such as in the data centre.
- Observance and maintenance of the physical security of rooms and offices where PC's and/or critical information processing equipment is located needs to be a paramount consideration. For example, do not house critical equipment in publicly accessible locations, close to windows, in areas where theft is a high risk. Locate servers and business critical equipment in locations with adequate environmental and fire controls.
- Access to information processing systems will only be allocated to staff following any required legal/MyTutor checks. If required, usage policies will also need to be signed by staff.
- All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.
- Access to and knowledge of key fobs, door lock codes or access to keys for locks, are restricted to authorised personnel only and must not be shared with any unauthorised person.
- Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the location manager in line with professional best practice.
- If electronic door locks/key fobs are in use they must be issued to authorised staff on an individual basis, be fully registered to that individual and only used by that individual. The key fob must be deactivated immediately when no longer required and registration details updated accordingly.
- Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.

- All MyTutor/Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this procedure.
- Personal, special access visits from relatives or acquaintances of personnel are not permitted within secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure.
- Equipment should be sited to minimise unnecessary, unauthorised access into work areas. For example, refreshment units or office machinery designed for visitors should be placed in public accessible areas only.

5 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 that staff holds sufficient, relevant knowledge concerning the security of information and systems. Designated owners of systems, who have responsibility for the management of ICT systems and inherent information, need to ensure that all staff has been made aware of their responsibilities toward security. Designated owners of systems and information need to ensure they uphold the security policies and procedures.

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's assets, or an event which is in breach of MyTutor's security procedures and policies.

All MyTutor employees, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through IS30 Incident Reporting and Management Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of MyTutor.

MyTutor will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

7 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,

Term	Description
	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

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 (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.

Role or Team	Description
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.

9 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.

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

11.1Contributors, Reviewers, and Approvers

#	Role	Name	Comment
1	Approver— MyTutor	Bertie Hubbard	
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 Security Forum. It can be reviewed prior to date here. This will be set when the document is Released
2	Document Date	04Sep2020 08:36	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

11.3Document 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

11.4Version 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		

11.5Applied ISO27001 Controls

Control Ref	Title
A.7.1.1	Screening
A.7.2.2	Information security awareness, education and training
A.9.2.1	User registration and de-registration
A.9.2.2	User access provisioning
A.9.2.3	Privilege management
A.9.2.4	Management of secret authentication information of users
A.9.2.6	Removal or adjustment of access rights
A.9.4.1	Information access restriction
A.18.2.2	Compliance with security policies and standards