Physical and Environmental Infrastructure 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 has a large and complex ICT infrastructure. The foundation of this structure is the Data and Communications Network which is facilitated and supported by many types of hardware including extensive cabling and supporting systems installed throughout MyTutor's various buildings and offices.

Physical and environmental security often provides the first line of defence of information and information systems with what might be called geographic or area security, with equipment security and general controls to protect physical assets.

2 Scope

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

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

3 Purpose

These procedures define the requirements to ensure that MyTutor's critical or sensitive information processing facilities are in secure areas and protected by a defined secure perimeter. Appropriate security and controls provide protection against unauthorised access or damage to information available within processing facilities.

The following procedures are closely linked to and should be read and used in conjunction with the Network security procedures, Desktop PC Security procedures, Password policies, and Internet and email policies.

4 Procedures

4.1 Three spheres of principal control

There are three spheres of principal control that are available and when used in conjunction can supplement and enhance the overall assurance of MyTutor's physical and environmental infrastructure.

The three controls are:

- Physical
- Technical
- Procedural.

1. Physical controls rely on the presence of physical limitations to secure the perimeter or environment (Buildings and locations) containing information and information processing facilities. Stopping unauthorised people from entering/breaking into buildings (Fire escapes, back doors), the use of locks on offices, server rooms, other sensitive areas and the willingness to challenge those who aren't wearing badges. Further to this, what to do if something does go wrong e.g. there is a break in, a location suffers a fire or the power supply fails.

2. Technical security involves security measures that employ technology in some way. Usually they are related to computers and software techniques but can equally apply to technical locks such as tokens or biometric techniques such as finger prints. They can extend to hardware through locking of ports or to some other technological solution for a specific application (e.g. MyTutor's VPN).

3. Procedural security covers the rules, regulations and policies that an organisation puts in place to help reduce the risk of issues arising e.g. obligatory policies such as internet and email, password protection, PC and network security.

A layered approach using all three types of security provides the best solution. A set of controls need to be effectively implemented such as:-

- Controls getting into the site, buildings or locations (Procedural and physical.)
- A set of well drafted and effectively policed policies, of which staff are well aware. For example, staff are aware of where and how to store, send or copy sensitive information and ensure encryption is used if necessary (Procedural and technical.)
- Physical, technical and procedural controls surrounding access to information processing systems. For example Specific logons / access technology to ICT equipment, systems and applications.
- Physical, technical and procedural controls to ensure safety, security and integrity of information and locations e.g. fire procedures, power failures, eating and drinking, back-up equipment, location of critical equipment.
- Business continuity plans and disaster recovery plans must exist to counteract any loss of critical equipment, infrastructure and / or data.
- Maintenance contracts and service level agreements that incorporate, for example: antivirus software, encryption, security breach reporting mechanisms.

4.2 Physical and Environment Procedures

MyTutor Infrastructure equipment is maintained and installed across most MyTutor buildings and locations e.g. network cables in cupboards, network connection points, PC's and printers, servers,

internet routers. Access to computers and devices must be controlled using secure methods and procedures in order to prevent damage to MyTutor assets and reputation.

1. 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's personnel) to MyTutor locations. All visitors must be issued with an authorised MyTutor visitor's badge when signing in and upon leaving any badges issued should be collected to prevent access by the employee/visitor at a later date.

2. Staff should wear their MyTutor ID badges and visitors must wear the Visitor ID badges) if needed, which have been issued to them and they must be supervised at all times when visiting secure areas and leaving these areas. People who are not displaying ID badges should be challenged. Any person not known to 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.

3. 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 as required, such as in the data centre and should be periodically reviewed to ensure they are operating as intended.

4. 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.

5. MyTutor ICT equipment 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.

6. Desktop PC's, laptops and CTO which have not been provided by MyTutor but have been approved for use may be subject to the relevant security checks and procedures by the IT Department and Internal Audit.

7. All ICT equipment, data and communication networks must be installed and maintained according to the manufacturer's guidelines and in line with all relevant MyTutor policies and procedures.

8. All MyTutor PC's, laptops and CTO will be distributed and maintained to ensure the minimum standards of software and hardware integrity and security. This will include the correct security configuration and initial and regularly updated protection from viruses, spyware/malware.

9. Network Support staff working remotely must observe the same controls and procedures as when working within MyTutor campus in order to ensure security and integrity and to prevent loss and/or damage to MyTutor assets and reputation.

10. 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.

11. All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.

12. Maintenance of MyTutor equipment and infrastructure will be carried out by IT Department authorised staff.

13. 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.

14. ICT equipment should be taken off site only if permission for this has been agreed. Extreme care regarding loss, damage or theft needs to be employed whilst the equipment is off site. Staff must adhere to any relevant procedures and guidance regarding the use of and security of ICT equipment being used off site.

15. 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 especially in instances where there has been a change in personnel, for example staff leaving.

16. 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. Any key fobs that are not being used should be securely stored and a separate record maintained of these fobs.

17. Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.

18. Doors which provide access to ICT Network Infrastructure equipment must not to be left/wedged open unless for the purpose of taking delivery of new equipment, to accommodate the movement of existing equipment, transportation of maintenance or cleaning equipment – an authorised member of staff must be present at all times to supervise access when doors are left open.

19. All MyTutor/Contracted Cleaners must have and display appropriate identification as required and be made aware of the requirements within this procedure.

20. 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 as required.

21. Consideration and understanding of health and safety guidelines/procedures should be followed to ensure security, integrity and safety of MyTutor's data and communications infrastructure. Smoke detectors should be located within the areas housing critical system

and applications with fire-fighting equipment maintained and periodically tested. Local operations staff should be provided with basic training in the use of fire suppressant equipment.

22. If it is suspected that any of the above procedures have been broken or compromised, then the concern should be placed before a senior manager or use the Security Incident Form to report the matter.

23. A business continuity plan and disaster recovery procedures must be in place in the event of the loss of a part, or the whole MyTutor Data and Communications Network infrastructure. Procedural documentation must be regularly updated to include any changes/updates to existing procedures or processes involved.

24. Data and Communications Network Infrastructure Fault Tolerance and Redundancy procedures must be in place and tested for effectiveness on a regular basis. Procedural documentation must be regularly updated to include any changes or updates.

25. 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.

26. ICT property and equipment should be indelibly marked. A full inventory of assets and their location is maintained and can identify the importance of each item to assist in the case of items being lost or stolen. It can also aid the maintenance, disposal of equipment and ensure that confidential information and licensed software is properly removed from all devices.

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 contractor's 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, MyTutorwill 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
The 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
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		

Version	Status	Actions	Action By	Date Started

10.5 Applied ISO27001 Controls

Control Ref	Title
A.9.1.1	Access control policy
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.9.2.5	Review of user access rights
A.11.1.1	Physical security perimeter
A.11.1.2	Physical entry controls
A.11.1.3	Securing office, rooms and facilities
A.11.1.4	Protecting against external and environmental threats
A.11.1.5	Working in secure areas
A.11.1.6	Delivery and loading areas
A.11.2.1	Equipment siting and protection
A.11.2.2	Supporting utilities
A.11.2.3	Cabling security
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.11.2.5	Removal of assets
A.12.1.1	Documented operating procedures
A.12.2.1	Controls against malware