Third Party Connection 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 13.4 Version Control, and section 13 Document Control

Contents

1 Overview

MyTutor permits connections to Third Party organisations to promote partnership working, information sharing, service provision and support arrangements with Third Party organisations or service providers. This policy is specific to MyTutor's requirements when establishing new links between MyTutor and Third Party organisations and makes reference to MyTutor's additional security policies and procedures.

2 Scope

Third parties are defined as any individual or organisation not employed directly by MyTutor. It also includes suppliers who require access to MyTutor's network to provide remote support.

This policy applies to all existing and new permanent or temporary connections and applies to any connection agreement with a third party. Any sanctions and obligations specified within the contract may be imposed as part of the third party connection agreement.

3 Purpose

The purpose of this policy is to clarify the procedures and responsibilities with regard to initiating a new connection between MyTutor and a Third Party organisation or service provider in order to maintain confidentiality, integrity and availability.

4 Policy Statement

The overall security of MyTutor's infrastructure, systems and data takes precedence over any individual requirements for a Third Party connection.

A specific business purpose must exist and be defined for a Third Party connection to be considered. For each Third Party connection agreement, named lead persons responsible for the system and information concerned must be appointed by both MyTutorand the Third Party.

A risk assessment should be conducted, prior to implementation of any connection, to identify specific requirements. It will be the responsibility of MyTutor's named lead person to carry out the assessment. The risk assessment will consider:

- A description of the participants in the assessment.
- The type of access required and the data that needs to be available to the Third Party.
- The value and sensitivity of information and information systems that may be exposed to unauthorised access
- The threat and vulnerability (the risk) to information and information systems and the impact if the threat were to take place

- The controls required to protect information and information systems. An overview of the users
- How the Third Party organisation manages and controls information security
- Details of how the Third Party will secure their ICT equipment and networks
- The method of access required – physical and logical connectivity between information systems.
- Dates of when the access is required from and a cessation date if a temporary arrangement. If a permanent arrangement is required, then an annual review must be incorporated in the agreement.
- Security incident management
- Legal requirements affecting stakeholders
- A statement assessing and listing all risks.
- An overall conclusion

Any Third Party Organisation with which MyTutor enters into a connection agreement must be able to demonstrate compliance with MyTutor's information security policies and enter into binding agreements that specify the performance to be delivered and the remedies available in the event of non-compliance.

MyTutor's point of contact will:

- Have administrative responsibilities
- Approve a non-disclosure agreement in conjunction with Legal Services for any/or named individuals accessing the services/information provided by the connection.
- Be responsible for remote access provision
- Act as a point of liaison both with the Third Party and IT Service
- Be responsible for ensuring background checks (such as DBS and Baseline Personnel Security Standard) are made on individuals utilising services/information provided by the connection
- Ensure all relevant bodies are informed when the connection is no longer required

The Third Party point of contact will:

- Be responsible for managing all aspects of the connection on behalf of the Third Party.
- Be the primary point of contact and be able to provide accurate information on all aspects of the Third Party.
- Ensure that all Third Party users have received appropriate training and have under-gone appropriate background checks.

Third Party access to MyTutor's network potentially exposes MyTutor's infrastructure to risk and therefore there must be an agreement in place that assures MyTutor that any third party connection meets the security standards. The Third Party must consider and address:-

- A description of services and service level agreement.
- Reference to relevant MyTutor security policies and legislation.
- Requirements for asset protection and access control.
- Responsibilities and liabilities.
- Monitoring rights and reporting processes.
- Conditions for termination and renegotiation of agreements.

If a log of third party activity on MyTutor's network is required as part of the agreement, then the third party will need to retain this log for the period specified in the agreement. Remote access software must be disabled when not in use.

All Third Party access must be facilitated through a method of connection approved by MyTutor which provides protection to the satisfaction of the company. All Third Party access must be logged via the IT Department and duly authorised before being permitted onto MyTutor's network. Once authorisation has been obtained a time restrictive user name and password should be provided.

Changes to methods of connection must be clearly defined and agreed by MyTutor and the Third Party.

Third Parties and MyTutor must inform each other about any security incidents which may impact on the confidentiality, integrity or availability of the third party service or data provided by the service. Incidents originating within MyTutor must be handled in accordance with the 'Security incident management policy and procedures'. The range of security incidents which will require security awareness procedures include:

- Computers left unlocked when unattended
- Password disclosures
- Virus warnings/alerts
- Media loss
- Data loss/disclosure
- Misuse/loss/corruption/alteration of Personal information
- Physical security
- Missing correspondence
- Found correspondence/media
- Loss or theft of IT/information
- Misuse of IT equipment/facilities

Third Parties with whom MyTutor has a Third Party connection contract are permitted access only to systems and information related to that contract. All other access is prohibited. Any Third Party with access to sensitive MyTutor information must be cleared to the same security and human resources checks as MyTutor's staff.

5 Responsibilities

It is the responsibility of MyTutor and each Third Party to ensure that all sections of this policy are adhered to.

Should changes in the requirements of either, it is the responsibility of MyTutor and each Third Party to ensure that all sections of this policy are adhered to.

Should changes in the requirements of either MyTutor or the Third Party regarding the connection become apparent, such as:-

- Life span of the service
- Changes in the information required

- Changes in the type of connection
- Changes in any aspect of security
- Changes of key contacts
- Emergency handling procedures

Each party should notify the other as soon as possible and the respective connection agreement should be revised.

6 Compliance with legal obligations

MyTutor and Third Parties will abide by all UK legislation relating to information storage and processing including:

A full List is in the Legislation list.

- The Data Protection Act (2018)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- Privacy and Electronic Communications Regulations (2003)

MyTutor and Third Parties will also comply with any contractual requirements, standards and principles required to maintain the business functions of MyTutor including:

- Protection of intellectual property rights.
- Protection of MyTutor's records.
- Compliance checking and audit procedures.
- Prevention of facilities misuse.
- Relevant codes of connection to Third Party networks and services.

7 Compliance with MyTutor ICT Policies

Several of MyTutor's non-ICT and ICT specific policies need to be considered as relevant within the sphere of any Third Party connection policy.

A full list is in the Policy list

8 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.

MyTutor will take appropriate measures to remedy any breach of a third party connection agreement. If a breach/security incident relates to a Third Party, MyTutor reserves the right to immediately terminate the Third Party connection and, subject to the nature of the breach/security incident, seek compensation or take legal action. If it can be determined that the breach/security incident has been caused by an employee of the third party, MyTutor would retain the right to request the employer to remove their employee from their premises.

If the breach/security incident is determined to have been caused by an individual employed by MyTutor, the matter may be dealt with under the disciplinary process.

9 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

Term	Description
	occurring through unauthorised disclosure or access to controlled information
The Business	MyTutor classified as Private Limited Business
The Business 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's forum where information security matters are discussed and activities related to information security are co-ordinated.
ICT	ICT, or information and communications technology

10 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 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.

11 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.

12 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

13 Document Control

13.1 Contributors, Reviewers, and Approvers

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

13.2 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

#	Name	Variable	Description	Comment
				Forum. It can be reviewed prior to date here. This will be set when the document is Released
2	Document Date	04Sep2020 08:35	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

13.3 Document Access Control Categories

The access categories/classifications in use

#	Category (Classification)	Circulation	Comment
1	CONTROLLED	Can only be circulated to MyTutor's 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

13.4 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		

Version	Status	Actions	Action By	Date Started
		Final Release		
1.1	Released	Minor amendments		

13.5 Applied ISO27001 Controls

Control Ref	Title
A.6.1.2	Segregation of duties
A.7.1.2	Terms and conditions of employment
A.7.2.1	Management responsibilities
A.12.1.4	Separation of development, test and operational environments
A.15.1.2	Addressing security within supplier agreements
A.15.2.1	Monitoring and review of supplier services