MyTutor www.mytutor.co.uk

Supplier Security 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

This document specifies the requirements that must be met by contractors in the handling, management, storage and processing of information belonging to MyTutor or its partners.

2 Scope

This applies to all Suppliers that supply services to MyTutor where there is a risk to MyTutor and its customers.

3 Purpose

The purpose of this policy is to:

- Detail the requirements of MyTutor to ensure information security and data protection to MyTutor and its customers.

4 Policy Statement

4.1 Information Security

1. Information security is the preservation of confidentiality, integrity and availability of MyTutor's information. It may also include the authenticity, accountability, non-repudiation and reliability of MyTutor information depending on circumstances. Information risk means the risks to the security of MyTutor's information.

4.2 Objectives

1. MyTutor requires the security of its information to be maintained in order to ensure that MyTutor is able to rely on its information for its MyTutor needs and meets its statutory, regulatory and legislative policy obligations.

2. MyTutor is certified as compliant with ISO/IEC 27001 and applies security controls consistent with this certification, and as found in ISO 27002 and the Annex of ISO 27001.

4.3 Information Risk Assessment and Management

1. MyTutor uses its risk assessment methodologies (as detailed in Risk assessment and risk treatment methodology).

2. Residual information risks can only be accepted by MyTutor’s CIRO to agreed levels.
3. MyTutor does not accept information risks assessed at ‘medium-high’ or above.
4. MyTutor information risk appetite is ‘cautious’.

4.4 Legislative, Regulatory and Contractual Requirements

1. The management of MyTutor and other official information may engage obligations under the following legislation (note that this list is not exhaustive) Is listed in the Regulation Register

2. Any organisation accessing, processing, communicating or managing MyTutor’s information must do so such that MyTutor’s legal, policy and regulatory obligations are met.
3. Any processing of personal data outside the United Kingdom may only take place with the express permission of MyTutor’s CIRO and prior to the commencement of any such processing. Arrangements for data processing will form part of a contract between MyTutor’s and data processors.

4.5 Access to MyTutor’s Information, Information Assets and Information Systems

1. Anyone accessing MyTutor’s information and/or work in a MyTutor building must either hold or be prepared to apply for clearance. This entails identity, nationality and criminal record checks. Clearance obtained through other MyTutor departments may be accepted by the Lead MyTutor Security Manager. If access is required to information at higher levels of security classification, additional national security vetting checks may be required.
2. Access to information assets and systems will be the minimum necessary to achieve MyTutor purposes.
3. When the need to access MyTutor’s information, assets and systems ends, all MyTutor equipment (e.g. laptops, security passes, etc.) must be returned to MyTutor prior to the termination of a contract.
4. MyTutor may monitor the use of its information, information assets and information systems for lawful MyTutor purposes.
5. Anyone granted access to MyTutor information, information assets and systems must comply with the requirements of MyTutor’s Security Policies including its Acceptable Use Policy. Failure to comply with these policies and other relevant instructions may constitute a breach of contract and lead to termination or legal action.
6. Removable media (including laptops) may only be used to manage MyTutor’s information with the explicit consent of CIRO. Any removable media must be encrypted to a degree commensurate with the security classification of the information held within the removable media.
7. Supplier personnel may only enter MyTutor’s premises with an appropriate security pass issued by MyTutor and may only enter areas of MyTutor’s premises commensurate with their function and, where appropriate (for example, in security areas), escorted by MyTutor’s staff.

4.6 Information Security Management System Controls

1. Where a supplier is contracted to manage MyTutor's information, information assets or information systems, the supplier must ensure that an information security management system is employed to secure MyTutor's information, information assets or information systems is in place and complies with ISO/IEC 27001. Evidence must be provided to MyTutor of compliance with the standard, either through formal certification or otherwise to MyTutor's satisfaction before any of MyTutor's information, information assets or information systems are accessed by the supplier.
2. Suppliers must agree to permit and facilitate audits of all aspects of their information security management system by MyTutor and to address any findings of such audits in order to preserve the security of information to MyTutor's standards and requirements.
3. The transmission of information between MyTutor and a supplier must be encrypted to a level commensurate with the security classification of the information and to MyTutor's standards.
4. Live MyTutor data and information may not be used for test purposes. Data and information to be used for test purposes must be sanitised, scrambled or otherwise rendered in such a way that no live MyTutor data or information can be reconstructed from that used for test purposes.
5. MyTutor information may not be copied by any supplier other than as far as is necessary for providing an agreed service to MyTutor
6. Suppliers must have a security incident reporting process in place to a standard and design acceptable to MyTutor to ensure that any incidents involving MyTutor's information are immediately reported to MyTutorSuppliers must agree to undertake any remedial action required by MyTutor and ensure that this is implemented in an auditable way.
7. A supplier holding MyTutor's data on MyTutor's behalf must have in place processes to ensure that critical MyTutor information held by them can be promptly and efficiently recovered following an emergency.

.

5 Supplier Data Protection Guidelines

The Following Guidelines issued by the UK Information Commissioners Office will be used for all suppliers that act as a processor for personal data.

1. The processor must only act on the written instructions of the controller (unless required by law to act without such instructions); including when making an international transfer of personal data.
2. The processor must ensure that people processing the data are subject to a duty of confidence;
3. The processor must take appropriate measures to ensure the security of processing;

4. The processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
5. The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
6. The processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
7. The processor must delete or return all personal data to the controller as requested at the end of the contract; and
8. The processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
9. The controller will state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and reflect any indemnity that has been agreed.
10. The Processor only act on the written instructions of the controller (Article 29);
11. The Processor cannot use a sub-processor without the prior written authorisation of the controller (Article 28.2);
12. The Processor will co-operate with supervisory authorities (such as the ICO) in accordance with Article 31;
13. The Processor will ensure the security of its processing in accordance with Article 32;
14. The Processor will keep records of its processing activities in accordance with Article 30.2;
15. The Processor will notify any personal data breaches to the controller in accordance with Article 33;
16. The Processor will employ a data protection officer if required in accordance with Article 37; and
17. The Processor will appoint (in writing) a representative within the European Union if required in accordance with Article 27.

5.1 The Processor will be aware of

1. The Processor may be subject to investigative and corrective powers of supervisory authorities (such as the ICO) under Article 58 of the GDPR;
2. The Processor if it fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR;
3. The Processor if it fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and
4. The Processor if it fails to meet its GDPR obligations it may have to pay compensation under Article 82 of the GDPR.

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
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.

Term	Description
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
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
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 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

Role or Team	Description
	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

11.1 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 Security Forum. It can be reviewed prior to date here. This will be set when the document is Released
2	Document Date	15Sep2020 15:33	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

11.3 Document Access Control Categories

The access categories/classifications in use

#	Category (Classification)	Circulation	Comment
1	MyTutorInternal	Can only be circulated to MyTutor personnel, and selected approved MyTutorpartners/third party suppliers	
2	MyTutor Edit	“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 polices		
1.0	Released	Reviewed and Amended for Final Release		

11.5 Applied ISO27001 Controls

Control Ref	Title
A.7.1.1	Screening
A.7.1.2	Terms and conditions of employment
A.7.2.2	Information security awareness, education and training
A.8.1.4	Return of assets
A.14.2.7	Outsourced development
A.15.1.1	Information security policy for supplier relationships
A.15.1.2	Addressing security within supplier agreements
A.15.1.3	Information and communication technology supply chain
A.15.2.1	Monitoring and review of supplier services
A.15.2.2	Managing changes to supplier services