# Operational 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 | MyTutor 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 15.4 Version Control, and section 15 Document Control |
| | | |

# Contents


1 Overview 4
2 Scope 4
3 Purpose 4
4 Policy Statement 4
4.1 Information Security 4
4.2 Documentation 4
4.3 Change Management 5
4.4 Separation of Development, Test and Operational Facilities 6
4.5 Capacity Management 6
4.6 System Acceptance 6
4.7 Patching 7
4.8 Protection against malicious and Mobile Code 7
4.9 Controls against malicious Code 7
4.10 Controls against Mobile Code 8
4.11 Back-ups 8
4.12 Restores 9
4.13 Media Handling 9
4.14 Disposal of Media and Paper 10
4.15 Security of System Documentation 10
4.16 Information transfer policies and procedures 11
4.17 Event Logging 12
4.18 Network Security Management 13
5 Restrictions on software installation 14
6 Contact with special interest groups 14
7 Logging and monitoring 14
8 Clock synchronisation 14
9 Vulnerability and Release Management 14
10 Breaches of Policy 15
11 Definitions 16
12 Duties and Responsibilities for Information Security 17
13 Policy Review 17
14 References 18

15 Document Control 18
15.1 Contributors, Reviewers, and Approvers 18
15.2 Document Maintenance 18
15.3 Document Access Control Categories 19
15.4 Version Control 19
15.5 Applied ISO27001 Controls 20

# 1 Overview

MyTutor's implementation of an Information Security Management System (ISMS) is essential to ensuring the security, confidentiality, integrity and protection of data, information and ICT.

# 2 Scope

This scope of this policy extends to all departments, employees, contractors, vendors and partner agencies who utilise or who are responsible for the development, management/maintenance of information within MyTutor's ICT processing facilities.

# 3 Purpose

The purpose of this policy is to detail the requirements for the correct and secure use of MyTutor's information processing facilities with the aim of ensuring the protection of information and data through the implementation of an effective ISMS (Information Systems Management System) in accordance with the ISO 27002 standard, and to achieve certification against the requirements of ISO 27001.

# 4 Policy Statement

## 4.1 Information Security

1. Maintaining and managing MyTutor's ICT data and information processing facilities requires a comprehensive and robust policy. The ISO 27001 Information Security Management System (ISMS) standard process provides MyTutor with a framework and methodology which enables a focused and structured approach to achieving this.

All policies and procedures outlined in MyTutor's Information Security policy and ratified by MyTutor's top management must be referred to and adopted by all departments to establish and maintain professional good working practices and procedures for the management of an effective ISMS - vital to counter threats to the availability, integrity and confidentiality MyTutor's data and information.

There are a number of controls which must be in place if MyTutor is to achieve this:

## 4.2 Documentation

All MyTutor's operating procedures and system processes outlined in MyTutor's IT Security Policy must be documented.

Operating procedures must be documented to an appropriate level of detail for individuals/departments using them and should include the following areas:

- Processing and handling of information (information classification, confidentiality requirements)
- Backup procedures - Information Backup and Restore Procedures
- Work scheduling requirements (considering interdependencies, completion times, etc.)
- Instructions and guidance for handling errors
- Contact and reporting details in the event of unexpected operational issues
- Procedures for handling special outputs (e.g. special stationery like cheques, payslips)
- System restart and recovery procedures in the event of system failure
- Procedures for all 'housekeeping' functions
- Procedures for audit and assurance reviews

## 4.3 Change Management

Changes to the ICT infrastructure must only be undertaken by authorised personnel working in an IT function/capacity (Or contractors, vendors, etc. authorised by MyTutor) and are subject to auditable change management procedures where applicable.

Changes to MyTutor's ICT infrastructure and operational systems must be controlled with a formal, documented change control procedure. The change control procedure should include references to:

- A description and reason for the change
- Information about any testing phase(s)
- Impact assessment including security, operational etc.
- Formal approval process – managerial approval and authorisation prior to proceeding with changes which may have a significant impact
- Communication to all relevant people of the changes which includes:
- Advance communication/warning of changes
- Proposed schedules
- Description of reasonably anticipated outcomes provided to all relevant personnel
- Procedures for aborting and rolling back if problems occur
- Processes for planning and testing of changes, including fall-back (abort/recovery) measures
- Documentation of changes made and all the steps taken in the change management process
- Identification of significant changes and relevant risk assessments - including analysis of any potential impact and necessary countermeasures or mitigation controls
- Changes are logged in the slack channel.

All changes to the ICT infrastructure need to be assessed for impact on the security of data and information as part of standard risk assessments.

## 4.4 Separation of Development, Test and Operational Facilities

Development and test environments must be separated from live operational environments in order to reduce the risk of accidental changes, configuration/data incompatibilities and unauthorised access. Development and live environments must be segregated by the most appropriate controls including:

- Running on separate computer/systems
- Running on different domains
- Use of test/temporary usernames and passwords

Where practical, separation of duties should be maintained to ensure no one individual can gain unacceptably high levels of access to MyTutor's ICT systems and information processing facilities.

## 4.5 Capacity Management

The IT Department must monitor the capacity demands of MyTutor's systems and make projections of future capacity requirements so that adequate power and data storage requirements can be fulfilled.

Utilisation of key system resources must be monitored so that additional capacity can be brought on line when required.

These include:

- File/storage servers (Cloud or otherwise)
- Domain/Network infrastructure devices and equipment
- E-mail/web servers
- Printers

Increases in MyTutor's business activities and staffing levels must also be monitored to allow for extra facilities which may be required e.g. number of available workstations etc.

## 4.6 System Acceptance

All departments must inform the IT Department, via the Service Desk, of any new software requirements or of any upgrades, service packs, patches or fixes required.

Appropriate levels of testing must be undertaken for new ICT systems, product upgrades, patches and fixes prior to acceptance and release into a live environment. The acceptance criteria must be clearly identified agreed and documented, and should involve appropriate levels of authorisation.

Software must be monitored for service packs, updates and patches which should be tested and applied as soon as possible when released and once it has been approved by the IT Department.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment which duplicates the 'live' operational system.

## 4.7 Patching

All security based service packs, patches and fixes supplied by 3rd party software vendors should be applied as soon as they become available.

All MyTutor's ICT system servers must have critical security patches applied as soon as they become available. All other patches and updates must be applied as appropriate. There must be a full record of which patches have been applied and when.

## 4.8 Protection against malicious and Mobile Code

The security and integrity of MyTutor's information and data, including all software applications, must be protected from malicious software (malware). Appropriate controls and user awareness procedures must be put in place to ensure MyTutor is protected.

## 4.9 Controls against malicious Code

Antimalware/Antivirus software must be installed and maintained on all workstations and servers and any other computing device which uses software to function and is capable of being scanned by Antimalware/Antivirus software. The software must be from an established vendor with consistent results in recognising and removing all types of malware. All updates must be installed as soon as they are available. A regular review of all business critical systems must be conducted to identify all software running on the systems. Any unauthorised files or software must be formally investigated and deleted as appropriate.

To protect systems from malware, users must not:

- Install software from any external source including the internet, CD / DVD-ROMs, USB memory sticks, etc. on their workstation.
- Add their own screensavers, desktop images, photos or utilities to the workstation.

All software must be approved and installed by the IT Department. Software must also be controlled to ensure compliance with licensing and other legal requirements.

Malware and viruses can be introduced through emails and users must be vigilant and MyTutor's guidelines on dealing with suspiCTOus emails and attachments. If there is uncertainty with the safety of particular emails or attachments, the IT Department should be contacted.

MyTutor must ensure that all email and attachments are checked for malware and viruses at the point of entry into the network.

More information is available in MyTutor's malicious Software and Anti-Virus Procedure and Internet and IInternet and Email Acceptable Use Policy.

## 4.10 Controls against Mobile Code

Mobile code is often found in web pages including:

- ActiveX
- Java
- JavaScript
- VBScript
- MSWord Macros

Certain websites rely on the use of these scripts which either run automatically or via user interaction with the site. MyTutor must protect its users and computers as much as reasonably possible by ensuring that, wherever possible, users are warned of the script to be run and by blocking connections and/or scripts to known 'bad' or harmful websites.

Mobile code must be prevented from entering the network with the exception of web sites that have been approved for use after the risk of the site has been assessed. Controls must be in place for the protection of all MyTutor's computers from harmful and unwanted running of mobile code.

## 4.11 Back-ups

MyTutor must ensure that regular backups of information, data and ICT systems configuration are routinely carried out to ensure MyTutor can recover from unforeseen events, system failure, accidental or deliberate loss of information or facilities - in line with Disaster Recovery Procedures outlined in Business Continuity Policy Manual.

All backup routines must be fully documented as described in Information Backup and Restore Policy.

To ensure all information and data is backed up, all employees must store their work on the network drive areas provided by The IT Department and not stored 'locally' on computer drives e.g. C: drive. The exception to this is during a loss of network connectivity when data must be temporarily stored locally until the network becomes available again. All users of portable devices e.g. laptops, tablets, PDA's, smart phones and USB memory sticks must ensure that data is not permanently stored on these devices and must transfer the data to MyTutor's network – more information on this is available in Laptop & Mobile Device Security Procedures.

All 3rd party / software vendors hosting or supplying services/facilities containing or handling MyTutor's information and data must ensure appropriate, secure backup routines and facilitate access for MyTutor's internal audit requirements when necessary - confirmation of this should be provided during the tender process.

Full back up documentation including a complete record of what has been backed up along with the recovery procedure must be stored at an off-site location in addition to the copy at the main site. This must also be accompanied by an appropriate set of media and stored in a secure area. The off-site location must be sufficiently remote to avoid being affected by any disaster which may take place at the main site, such as an online and protected storage cloud.

Critical paper files must be identified and backed up with either a scanned digital copy or complete photocopies stored at a remote location.

## 4.12 Restores

Full documentation of the recovery procedure must be created and stored. Regular restores of information from backup media must be carried out and tested to ensure the reliability of the backup media and restore process.

Retention periods for information and data must be defined and applied to the backup schedule planning. Long term backup and restore solutions need to be identified and applied wherever necessary.

## 4.13 Media Handling

Removable media such as USB data sticks, CD/DVDs, magnetic tapes, external hard drives etc., must be protected to prevent damage, theft or unauthorised access.

Documented procedures must be in place for backup media that are removed on a regular rotation from MyTutor's buildings and where/if appropriate. Backup media must be kept in a secure environment e.g. a fireproof safe in a lockable room/area. Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

Media being transported must be protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate, physical controls should also be used e.g. encryption or special locked containers for the secure transfer of Information.

## 4.14 Disposal of Media and Paper

Media which is no longer required must be disposed of safely and securely. Media containing sensitive or person identifiable information must be disposed of appropriately in accordance with the Record Disposal Policy and all existing disposal procedures within MyTutor.

Items that should be considered for secure disposal include:

- Paper documents
- Voice or other recordings
- Magnetic tapes
- Removable disks
- USB Memory sticks
- CD/DVD ROMs

All media for disposal must be completely erased using methods which negate the possibility of data recovery and reconstruction from devices or media.

The IT Department must be contacted for the secure disposal of ICT media and devices.

## 4.15 Security of System Documentation

All ICT system documentation must be protected from unauthorised access. This includes documentation that has been created by the IT Department or any other departmental IT employees (this does not include manuals that have been supplied with software). Examples of the documentation to be protected include descriptions of:

- Applications
- Processes
- Procedures
- Data structures
- Authorisation details

## 4.16 Information transfer policies and procedures

Processes and procedures and must be implemented to protect the transfer of information through all available methods and formats e.g. email, cloud, letter and fax etc.

Procedures must be designed to protect exchanged information against:

- Interception
- Copying
- Modification
- Misrouting
- Destruction
- Access
- Availability
- Loss

Information and data must be protected with appropriate controls based on the information's classification e.g. Confidential / Controlled. Https, VPN and TLS must be used where required. Authentication must be in place for access and identity verification on all internet and public facing systems enabling all communication paths to be encrypted ensuring privacy associated with all parties involved is retained;

a) the level of confidence each party requires in each other's claimed identity, e.g. through authentication;

b) authorization processes associated with who may approve contents of, issue or sign key transactional documents;

c) ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;

d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e) the level of trust required in the integrity of key documents;

f) the protection requirements of any confidential information;

g) the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;

h) the degree of verification appropriate to verify payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;

j) the level of protection required to maintain the confidentiality and integrity of order information;

k) avoidance of loss or duplication of transaction information;

l) liability associated with any fraudulent transactions;

m) insurance requirements.

Regulated and autoreactive use of electronic signatures by each of the parties involved in the transaction.

user's secret authentication information of all parties are valid and verified;

- the transaction remains confidential;
- privacy associated with all parties involved is retained;
- communications path between all involved parties is encrypted;
- protocols used to communicate between all involved parties are secured;
- ensuring that the storage of the transaction details is located outside of any publicly accessible
- environment, e.g. on a storage platform existing on the organizational intranet, and not retained
- and exposed on a storage medium directly accessible from the Internet;
- Where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures
- or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Formal agreements for the transfer of information between MyTutor and external organisations must be made and reviewed on a regular basis.

## 4.17 Event Logging

ICT system audit logs must be kept for a minimum of six months which record exceptions and other security related events. As a minimum, audit logs must contain the following information:

- System identity (Workstation name)
- User ID (employee number)
- Successful/Unsuccessful login
- Successful/Unsuccessful logoff
- Unauthorised application access

- Changes to system configurations
- Use of privileged accounts (e.g. account management, policy changes, device configuration)

Access to the logs must be protected from unauthorised access that could result in recorded information being altered or deleted. System administrators must be prevented from erasing or deactivating logs of their own activity. Access to logs should be provided for MyTutor's internal audit requirements when necessary.

Operational staff and system administrators must maintain a log of their activities. The logs should include:

- Back-up timings and details of exchange of backup tapes
- System event start and finish times and who was involved
- System errors (what, date, time) and corrective action taken

The logs should be checked regularly to ensure that the correct procedures are being followed.

## 4.18 Network Security Management

The management and security of the data and communications network is critical to ensuring the integrity and security of MyTutor's systems and data. The following controls must be applied:

- Operational responsibility for networks should, wherever possible, be separated from computer operations activities
- There must be clear responsibilities and procedures for the management of remote equipment and users
- Where appropriate, controls must be put in place to protect data passing over the network e.g. encryption

The network architecture must be documented and stored with configuration settings of all the hardware and software components that make up the network.

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption must be used on the network to protect information and data and to prevent information being intercepted.

# 5 Restrictions on software installation

- Employees may not install software on MyTutor's computing devices
- operated within the MyTutor network and cloud infrastructure.
- Software requests must first be approved by the requester's manager and then be made
- to the Information Technology department or Help Desk in writing or via email.
- Software must be selected from an approved software list, maintained by the Information
- Technology department, unless no selection on the list meets the requester's need.
- The CEO will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

# 6 Contact with special interest groups

MyTutor should ensure that the they on the alerting lists of all software, Cloud and OS vendors and suppliers and NCSC to ensure that MyTutor is up to date on information security issues.

# 7 Logging and monitoring

Events are recorded using Amazon tools AWS Config, Amazon Cloud Watch and other methods for monitoring the use of super user passwords so that System administrator and system operator activities are logged and the logs protected and regularly reviewed, recording user activities, exceptions, faults and information security events.

# 8 Clock synchronisation

Clock synchronisation is in the AWS cloud.

# 9 Vulnerability and Release Management

For many systems, it will be appropriate to enable automatic updates. This is the recommended method for patching personally-owned devices, most workstations, and may also be appropriate for some servers.

Whereas in other cases, applying patches manually may be preferable.

Wherever:

• a vendor / developer releases a patch to fix a security vulnerability, or:

• a vulnerability is identified (e.g. via a network scan)

• a requirement exists to run software unsupported by the vendor / developer

- Then the issue must be addressed within 30 days or a dispensation must be obtained from the CEO

Where the risk is assessed as critical (e.g. where attacks on MyTutor are known to be plausibly imminent or taking place) then the vulnerability must be addressed immediately.

A risk based decision will be made by the CEO.

In most cases, installing an update or security patch is the preferred approach to address a vulnerability.

Where updating or installing patches is not desirable or possible, within the 30-day timeframe, a risk-based approach must be used to determine whether appropriate mitigation measures can be put in place, or alternatively, whether the risk is already mitigated to an acceptable level. This will involve assessing the likelihood of the vulnerability being exploited and the resulting impact on MyTutor.

Mitigations may include physical or logical separation from the network; The CEO/Security officer Will advise mitigations (if any) can reduce the risk to an acceptable level.

Vulnerabilities that cannot be mitigated to an acceptable level of risk must be promptly escalated to the CEO/Security Officer, who may approve a dispensation for the vulnerability, which will be entered into the risk register.

If none of the above measures are viable then the insecure system should be blocked from accessing MyTutor's data network until an acceptable solution is available.

Systems must be actively checked to ensure that all required patches are installed; this may involve manual checks, or automated methods (e.g. a monitoring agent installed on individual systems, reporting to a management station). Whichever method is used, all systems must be checked on a regular basis to confirm they are patched as intended, and it is strongly recommended this be done at least every 30 days.

# 10 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 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.

# 11 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[1] 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[2] |
| MyTutor Personnel | Includes all MyTutor employees as well as all temporary staff, contractors, consultants and any third party with whom special arrangements have been |

[1] If found and held accountable for a security breach by a Court of Law or by the Information Commissioners Office, potentially both the individual and corporate entity may be subject to sanction.

| Term | Description |
|---|---|
| | 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 |

# 12 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. |

# 13 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.

# 14 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 |

# 15 Document Control

## 15.1Contributors, Reviewers, and Approvers

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

## 15.2 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 |

| # | Name | Variable | Description | Comment |
|---|---|---|---|---|
| | | | | be set when the document is Released |
| 2 | Document Date | 04Sep2020 08:38 | 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 |

## 15.3 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 |

## 15.4 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 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 15.5 Applied ISO27001 Controls

| Control Ref | Title |
|---|---|
| A.6.1.2 | Segregation of duties |
| A.8.3.1 | Management of removable media |
| A.8.3.2 | Disposal of media |
| A.12.1.1 | Documented operating procedures |
| A.12.1.2 | Change management |
| A.12.1.3 | Capacity management |
| A.12.1.4 | Separation of development, test and operational environments |
| A.12.2.1 | Controls against malware |
| A.12.3.1 | Information backup |
| A.13.1.1 | Network controls |
| A.13.2.1 | Information transfer policies and procedures |
| A.14.1.2 | Securing application services on public networks |
| A 14.1.3 | Protecting application services transactions |
| A.14.2.9 | System acceptance testing |