MyTutor www.mytutor.co.uk

Desktop/Laptop/Server PC Security and malicious Software and Anti Virus 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 11.4 Version Control, and section 11 Document Control

Contents

1 Overview 3

2 Scope 3

3 Purpose 3

4 Procedures 3

4.1 Commissioning and Replacement 3

4.2 Configuration 4

4.3 Location 5

4.4 Use 5

4.5 Maintenance 6

4.6 Disposal 6

4.7 Guidelines 6

5 malicious Software and Anti Virus Procedure 7

5.1 Product Selection 7

6 Breaches of Policy 8

7 Definitions 9

8 Duties and Responsibilities for Information Security 10

9 Policy Review 10

10 References 11

11 Document Control 11

11.1 Contributors, Reviewers, and Approvers 11

11.2 Document Maintenance 11

11.3 Document Access Control Categories 12

11.4 Version Control 12

11.5 Applied ISO27001 Controls 13

1 Overview

MyTutor is reliant on the use of ICT equipment across all areas of its business. Devices such as desktop, laptop, notebook and tablet PC's are provided for use by those who require them to carry out their duties. All employees have a duty to ensure that appropriate levels of security are applied to all PC's used in the office environment.

2 Scope

This applies to all PC/Laptop and server builds for internal and customer use.

3 Purpose

The purpose of these procedures is to ensure that PC's in a Business environment are used, configured and managed in a secure and safe way and to identify and describe the steps required to achieve and maintain this.

4 Procedures

ICT equipment such as desktop, laptops, notebooks and tablet PC's are all capable of being used in the office environment over long periods on a daily basis.
The scope of these procedures cover:

- Any desktop, laptop, tablet, notebook (mobile device) PC.
- Configured with a Windows 10 operating system and has a desktop image.
- Provided by MyTutor.
- Predominantly used in the office environment.
- That is or can be connected to MyTutor’s Network.

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

Normal, everyday use of PC's provided by MyTutor for potential use within the office environment requires the following security considerations:

4.1 Commissioning and Replacement

- All requests for the purchasing new Desktop PC's are placed through the IT Department.
- Every new PC ordered from the approved supplier of MyTutor is provided with MyTutor’s asset tag number – this number is used to name the PC and is also recorded against the

computer for any fault calls or installation/maintenance requests made through the Service Desk or call logging system.
- Except where a workplace assessment or business need dictates otherwise, computers are replaced using the 'standard' approved hardware and software specification as identified by and existing on the approved software and hardware list created by IT Department.
- All new PC's are (Will be as of [dd/mm/yyyy]) marked using etching type stencils with the name "MyTutor's Name" on both the PC monitor (screen) and main computer case.
- The computer asset number is recorded in the central hardware inventory database. The life of the PC from commissioning to disposal can be tracked and recorded.

4.2 Configuration

- All MyTutor's PC's are supplied to users with a preconfigured standard Build Operating System image which the IT Department has developed in line with NCSC guidelines.
- Differing departmental requirements result in department specific applications being layered on top of the standard image. In terms of security; all computers connected to MyTutor's network domain will all have the same level of security applied across all areas.

- All MyTutor's Desktop PC's are subject to the following configuration which ensures PC's are added to the network and have the correct security configuration settings applied:

    - All MyTutor's PC's use the build to NCSC guidelines Operating Systems.
    - New Desktop PC's will have the approved "standard" image loaded by the IT Department. The configuration of the Desktop some changes which may be necessary for optimisation of the operating system.
    - PC's can only be added to MyTutor's Domain and a computer account created by an authorised IT Department account that has sufficient access permissions to do so.
    - Newly commissioned Desktop/laptop/tablet PC's are added to MyTutor's Domain using an asset tag number with a prefix relevant to the type of PC.
    - MyTutor's PC's are protected from viruses and spyware/malware using MyTutor's Endpoint. Virus definition files will be released across the network as and when required.
    - Users are not able to install un-approved software, even for a trial or demonstration.
    - Following the adding of a PC to the Domain, the security settings for the PC are applied and enforced automatically, immediately on "boot-up" of the computer.
    - Screen savers and desktop will be supplied and approved by the IT Department and cannot be changed by users.
    - Software firewalls built into the operating system must be enabled.
    - All software is regularly checked on all devices and deleted if no longer needed.
    - All user accounts on systems are reviewed and checked if they are needed
    - It is part of our off-boarding procedure to delete all accounts associated with that employee

N.B Desktop PC's which have not been provided by MyTutor but have been approved for use will be subject to the relevant security checks and procedures by the IT Department.

4.3 Location

Desktop/laptop/notebook/tablet PC's which are used by MyTutor’s employees, partner agencies, contractors and vendors are located across many sites and buildings.

The wide nature of access to many of these buildings and locations requires increased vigilance and awareness of the need for Desktop PC's to be secure and protected from unauthorised access, theft, physical damage, and tampering.

Care and professional judgement to protect information and data should be taken in using computers which are located and positioned where:

- PC screen/s may be visible to members of the public/service users.
- There is a danger of physical damage to a PC e.g. dropping, water, electrical.
- PC's may be subject to interference e.g. strong electromagnetic sources.
- PC's may easily be picked-up and / or stolen in obscured, low visible, non-staffed areas.

It is important to observe and maintain the physical security of rooms and offices where PC's are located.

MyTutor’s employees, partner agencies, contractors and vendors must be mindful of the potential for unauthorised access and viewing of MyTutor’s data and Information by members of the public/service users and take appropriate steps to avoid or prevent this.

4.4 Use

MyTutor’s PC's may only be used by authorized parties for authorized business of MyTutor or purposes in accordance with MyTutor’s Acceptable Use Policy and associated security policies.

All users of MyTutor’s Desktop/laptop/notebook/tablet PC's must ensure at all times that:

- Account logon and system passwords are kept private and not shared, displayed or communicated to anyone else.
- MyTutor’s information and data must not be saved to PC hard drives – in the event of MyTutor’s network being unavailable, advice should be sought from the IT Department.
- Sensitive and personal data must not be saved on the PC's hard drive under any circumstances.
- Data and Information saved to portable devices via a PC must only be copied to a portable device which is encrypted in accordance with MyTutor’s Encryption Policy.
- Screens/computers must be locked by users when away from the computer.
- PC's are not removed from their location without line management and/or approval from the IT Department.
- Unauthorised, non-standard equipment is not plugged-in or inserted into the computer.
- Software is not installed on the PC by unauthorised staff – any software installed must be (or going through the process of being) placed on the approved software list.
- PC's must not be mishandled, wilfully damaged or tampered with in any way – this includes taking off the PC case cover, or removing of any screws or fixings.

- Any suspicious or unknown equipment near or around PC's is reported to the IT Department.
- PC's are logged off and shut down when not in use for extended periods (i.e. overnight) and monitors are powered off.

Please note:
Any warnings visible on screen from the [Antivirus] software about identified/detected threats from viruses/malware should be reported to the IT Department.

4.5 Maintenance

- All PC maintenance whether routine or major is carried out by IT Department authorised staff and our authorised third parties.
- Only staff working within an ICT function (Or persons authorised by the IT Department) may perform maintenance, install applications/software or make system configuration changes to PC's. Staff may occasionally be requested to assist while under the supervision and authorisation of the IT Department as appropriate.
- A standard base configuration is installed on all MyTutor's PC's. Any variations and additions must be agreed by the IT Department and the Security/Business Continuity Manager.
- PC's are protected against malicious code in accordance with MyTutor's malicious software and anti-virus Procedure.
- PC's are maintained in accordance with all relevant policies and procedures within MyTutor.

4.6 Disposal

MyTutor operates a PC replacement programme. Computers which reach or exceed the term can, if required, be scheduled for replacement and disposed of through MyTutor's ICT disposal procedures.

Without exception, any computer or device which is used for the handling or creation of MyTutor data must be secured and is subject to all the relevant policies and procedures specific to the security of ICT equipment and its use.

These procedures should be read in conjunction with the Laptop and mobile device security procedures and the Security Incident management policy and procedures.

4.7 Guidelines

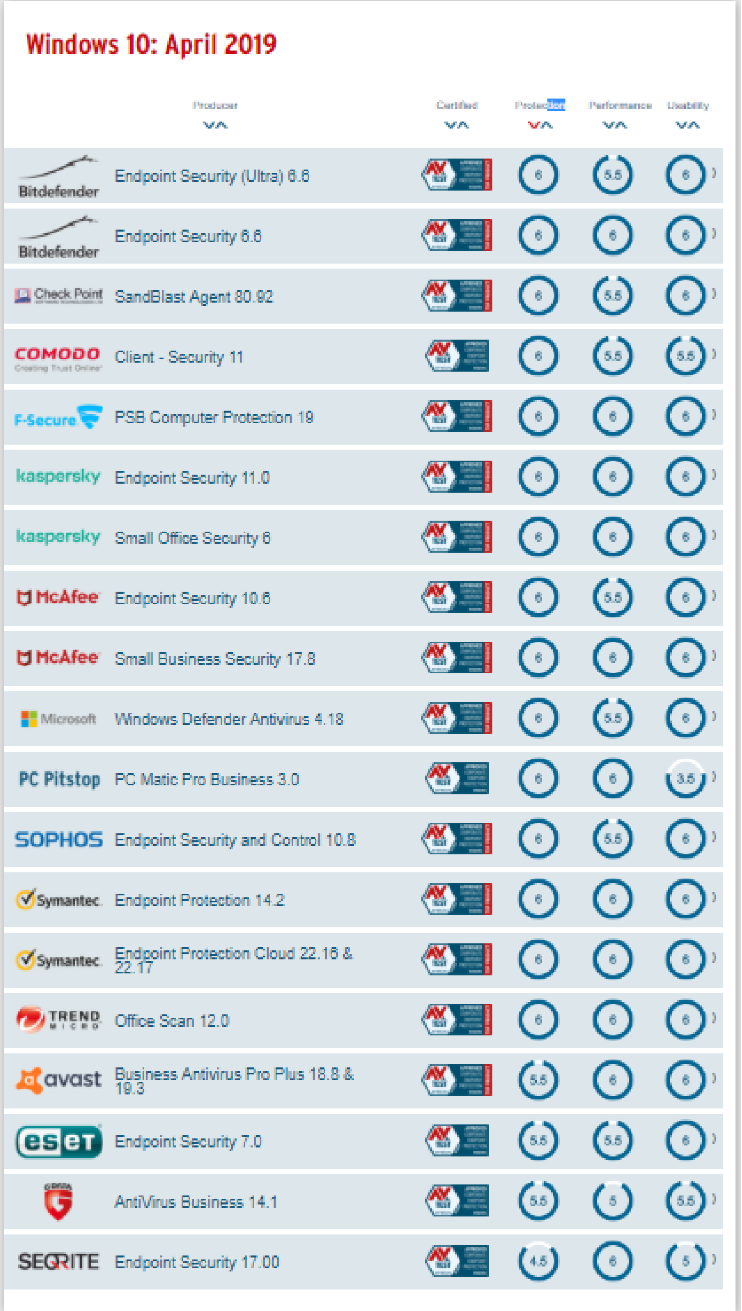
Guidelines for the security of all build must be taken from the NCSC website
https://www.ncsc.gov.uk/collection/end-user-device-security
https://www.ncsc.gov.uk/collection/developers-collection
https://www.ncsc.gov.uk/blog-post/securing-office-365-with-better-configuration
https://www.ncsc.gov.uk/blog-post/applying-the-cloud-security-principles

5 malicious Software and Anti Virus Procedure

5.1 Product Selection

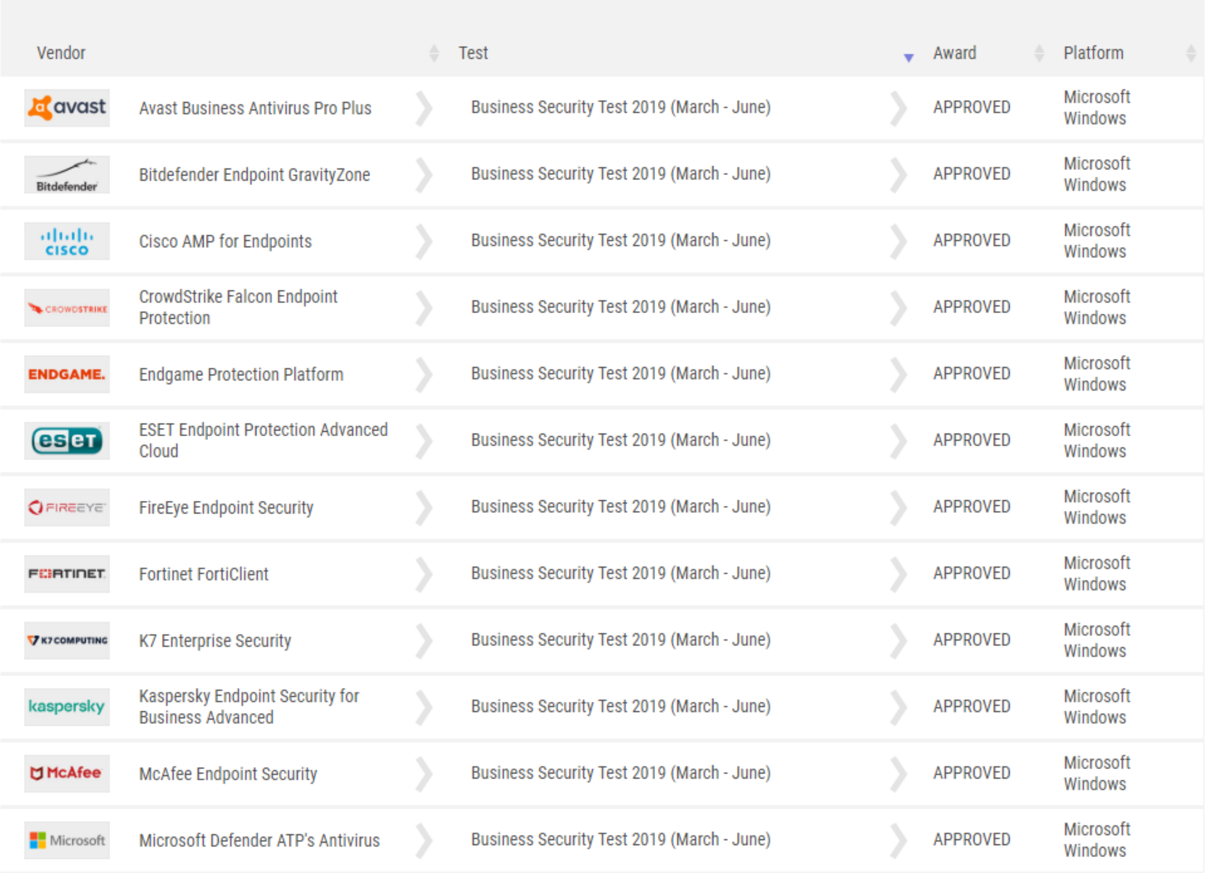
Virus Product must be used and rank well in the following test sites.

https://www.virusbulletin.com/testing/vb100/
https://www.av-comparatives.org/
https://www.av-test.org/en/antivirus/home-windows/



Windows 10: April 2019

Producer		Certified	Protection	Performance	Usability
Bitdefender	Endpoint Security (Ultra) 6.6	AV TEST	6	5.5	6
Bitdefender	Endpoint Security 6.6	AV TEST	6	6	6
Check Point	SandBlast Agent 80.92	AV TEST	6	5.5	6
COMODO	Client - Security 11	AV TEST	6	5.5	5.5
F-Secure	PSB Computer Protection 19	AV TEST	6	6	6
kaspersky	Endpoint Security 11.0	AV TEST	6	6	6
kaspersky	Small Office Security 6	AV TEST	6	6	6
McAfee	Endpoint Security 10.6	AV TEST	6	5.5	6
McAfee	Small Business Security 17.8	AV TEST	6	6	6
Microsoft	Windows Defender Antivirus 4.18	AV TEST	6	5.5	6
PC Pitstop	PC Matic Pro Business 3.0	AV TEST	6	6	3.5
SOPHOS	Endpoint Security and Control 10.8	AV TEST	6	5.5	6
Symantec	Endpoint Protection 14.2	AV TEST	6	6	6
Symantec	Endpoint Protection Cloud 22.16 & 22.17	AV TEST	6	6	6
TREND MICRO	Office Scan 12.0	AV TEST	6	6	6
avast	Business Antivirus Pro Plus 18.8 & 19.3	AV TEST	5.5	6	6
eset	Endpoint Security 7.0	AV TEST	5.5	5.5	6
G DATA	AntiVirus Business 14.1	AV TEST	5.5	5	5.5
SEQRITE	Endpoint Security 17.00	AV TEST	4.5	6	5



Vendor		Test	Award	Platform
avast	Avast Business Antivirus Pro Plus	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
Bitdefender	Bitdefender Endpoint GravityZone	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
cisco	Cisco AMP for Endpoints	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
CROWDSTRIKE	CrowdStrike Falcon Endpoint Protection	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
ENDGAME.	Endgame Protection Platform	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
eset	ESET Endpoint Protection Advanced Cloud	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
FIREEYE	FireEye Endpoint Security	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
FORTINET	Fortinet FortiClient	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
K7 COMPUTING	K7 Enterprise Security	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
kaspersky	Kaspersky Endpoint Security for Business Advanced	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
McAfee	McAfee Endpoint Security	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows
Microsoft	Microsoft Defender ATP's Antivirus	Business Security Test 2019 (March - June)	APPROVED	Microsoft Windows

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.
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	A 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 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

#	Name	Variable	Description	Comment
				Released
2	Document Date	15Sep2020 15:37	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	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

11.4 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		
1.2	Released	Minor amendments		

Version	Status	Actions	Action By	Date Started

11.5 Applied ISO27001 Controls

Control Ref	Title
A.6.2.1	Mobile device policy
A.8.1.1	Inventory of assets
A.8.1.3	Acceptable use of assets
A.8.2.3	Handling of assets
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.9.3.1	Use of secret authentication information
A.9.4.2	Secure log-on procedures
A.9.4.3	Password management system
A.9.4.4	Use of privileged utility programs
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.11.2.5	Removal of assets
A.11.2.6	Security of equipment and assets off-premises
A.11.2.7	Security disposal or re-use of equipment
A.11.2.8	Unattended user equipment
A.11.2.9	Clear desk and clear screen policy
A.12.1.1	Documented operating procedures
A.12.2.1	Controls against malware
A.18.2.2	Compliance with security policies and standards