


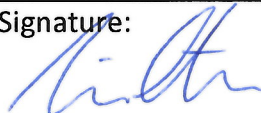




**NUFFIELD  
DEPARTMENT OF  
SURGICAL SCIENCES**



**UNIVERSITY OF  
OXFORD**

**NDS Information Security Policy**

**Effective date: 1<sup>st</sup> Feb 2013**

Author	Name: Tim Cranston	Title: IT Officer
	Signature: 	Date: 31/01/2013
Reviewed by	Name: Tania Boyt	Title: Business Manager
	Signature: 	Date: 31/01/2013
Reviewed by	Name: Tracy Tompkins	Title: Deputy Business Manager
	Signature: 	Date: 31/01/13
Reviewed by	Name: Sylvain Phaneuf	Title: IMSU Systems Manager
	Signature: 	Date: 31.1.2013
Authorised by	Name: Freddie Hamdy	Title: Head of Department
	Signature: 	Date: 1/2/2013

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
---	-----------------------------	--

1.1	Introduction .....	4
1.2	Policy Statement .....	4
1.3	Scope.....	4
1.4	Definitions.....	4
1.5	Abbreviations and Acronyms.....	5
1.6	Roles and responsibilities: .....	5
1.7	Information Security Policy Ownership and Responsibility .....	5
1.8	Audit and review.....	6
1.9	Regulatory and Legislative Requirements .....	6
1.10	Internet and email usage.....	6
1.11	Authentication and Authorisation.....	7
1.12	Building Security .....	7
1.13	Network and Systems IT Security .....	8
1.14	Computers, Software and Hardware.....	8
1.15	Information Handling .....	8
1.16	Application Development and Validation .....	9
1.17	Back-up and Archiving: .....	9
1.18	Projects .....	10
1.19	Encryption.....	10
1.20	Remote Access and Home Working .....	10
1.21	Disaster Recovery and Business Continuity .....	11
1.22	Sanctions .....	11
1.23	Risk Assessment .....	12
1.24	Connected Policies and References .....	12
1.25	Annex A.....	13
1.26	Annex B.....	14

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

## 1.1 Introduction

- 1.1.1 This policy is designed to be the overarching Information Security Policy for the Nuffield Department of Surgical Sciences (NDS) and is the primary policy under which all other technical and security policies reside. Annexe B provides a list of all of the NDS's technical policies that this Policy supports.
- 1.1.2 The policy is designed to ensure that the NDS will comply with all relevant compliance legislation in respect of information security. The policy will describe specific NDS rules on information security and reference any subservient policies that will describe policy in more detail. Annexe A provides a list of all the relevant security legislation to which this Policy makes specific reference.

## 1.2 Policy Statement

- 1.2.1 The purpose and objective of this Information Security Policy is to protect the NDS's information assets from all threats, whether internal or external, deliberate or accidental, it also describes measures to ensure business continuity, minimise damage and maximise return on investment.
- 1.2.2 Information will be protected from a loss of: confidentiality, integrity and availability.

## 1.3 Scope

- 1.3.1 This policy is intended for all staff and any visitors using the NDS IT systems, data or any other information asset.
- 1.3.2 For the purposes of this Policy the term "staff" will be taken to mean paid employees, authorised associate members, honorary members and academic visitors to the NDS.

## 1.4 Definitions

To avoid ambiguities, particular terminology is used when explaining the policies:

- **MUST:** This word, or the terms "REQUIRED" or "SHALL", means that the item is an absolute requirement.
- **MUST NOT:** This phrase, or the phrase "SHALL NOT", means that the item is absolutely prohibited.
- **SHOULD:** This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED", means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implication should be understood and the

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

case carefully weighted before implementing any behaviour described with this label.

## 1.5 Abbreviations and Acronyms

FIPS	Federal Information Processing Standard
HFS	Hierarchical File Server
ICT	Information, Communications & Technology
ICTC	Information, Communications & Technology Committee ( <a href="http://www.admin.ox.ac.uk/ictc/">http://www.admin.ox.ac.uk/ictc/</a> )
IMSU	Information Management Services ( <a href="http://www.imsu.ox.ac.uk/">http://www.imsu.ox.ac.uk/</a> )
IT	Information Technology
ITS	Oxford University's IT Services ( <a href="http://www.it.ox.ac.uk/">http://www.it.ox.ac.uk/</a> )
MSD	Medical Sciences Division
NDS	Nuffield Department of Surgical Sciences
SOP	Standard Operating Procedure
TSM	Tivoli Storage Manager
VPN	Virtual Private Network

## 1.6 Roles and responsibilities:

- 1.6.1 The Policy is approved by the Head of Department of the NDS, currently Professor Freddie Hamdy.
- 1.6.2 The Information Security Manager for the NDS, is the Business Manager, currently Tania Boyt.
- 1.6.3 The NDS Executive Committee is the designated owner of the Information Security Policy.
- 1.6.4 The IT Officer for the NDS is currently Tim Cranston.
- 1.6.5 The Data Controller for the NDS is the named University of Oxford Data Controller.
- 1.6.6 Council has ultimate responsibility for information security within the University. More specifically, it is responsible for ensuring that the University complies with relevant external requirements, including legislation.
- 1.6.7 For the purposes of the Data Protection Act 1998 NDS is registered under the University of Oxford, registration number: Z575783X

## 1.7 Information Security Policy Ownership and Responsibility

- 1.7.1 The roles and responsibilities of the designated Information Security Manager are to manage information security and to provide advice and guidance on implementation of the Information Security Policy.
- 1.7.2 The Designated Owner of the Information Security Policy has final responsibility for maintaining and reviewing the Information Security Policy.

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

1.7.3 It is the responsibility of all line managers to implement the Information Security Policy within their area of responsibility.

1.7.4 It is the responsibility of each member of staff to adhere to the Information Security Policy.

## **1.8 Audit and review**

1.8.1 The Information Security Manager will be responsible for arranging and monitoring regular audits of all aspects of the Information Security Policy. The results of audits will be recorded and logged. Audits will be carried out no less than annually.

1.8.2 The Information Security Policy will be reviewed annually by the Information Security Manager and approved by the NDS Executive Committee.

## **1.9 Regulatory and Legislative Requirements**

1.9.1 The Information Security Policy is designed to ensure that all regulatory and legislative requirements will be met.

1.9.2 Annexe A provides a list of relevant legislation and guidance to which this Policy refers.

## **1.10 Internet and email usage**

1.10.1 Internet access is provided via the University's network, which is managed by IT Services. IMSU's network infrastructure connects the NDS to the University's network.

1.10.2 All users of the NDS network are required to be aware of the University of Oxford Rules on Computer Use. New staff will be emailed these rules as part of the induction process. These rules are also available at <http://www.ict.ox.ac.uk/oxford/rules/>.

1.10.3 All users of the NDS network are required to be aware of the JANET acceptable Use Policy which details how University members are expected to use the network. New staff will be emailed these rules as part of the induction process. These rules are also available at <http://www.ja.net/services/publications/policy/aup.html>.

1.10.4 All members of staff are expected to have read, understood and to adhere to the IMSU Security Policy. The IMSU Security Policy will be issued in electronic format to all new staff and every new starter will be required to meet with the IT Officer and have an IT induction before using the IT systems.

1.10.5 The use of email within the NDS is controlled by IT Services and is covered by the University's ICTC regulations 1 of 2002 (with subsequent amendments) and available

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

at <http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml> (Regulation 7 is particularly relevant to the transmission of electronic mail) and is overseen by the IT Officer.

- 1.10.6 Breaches of any policy rules will in the first instance be reported to the line manager and then a record of the breach should be passed to the IT Officer.

### **1.11 Authentication and Authorisation**

1.11.1 All members of staff will be issued with a University Card. This card will give the NDS the authority for the member to become a user of the IMSU computer network and to use the University of Oxford Nexus email system. The rights and responsibilities of University of Oxford card holders are detailed at:

<http://www.admin.ox.ac.uk/card/>.

- 1.11.2 Staff may apply for a computer account subject to line manager approval. Application will be made by the NDS IT Officer and is processed by the IMSU administrative team. Passwords and computer accounts must not be shared or disclosed to any third party.
- 1.11.3 Computer accounts will only allow access to shared departmental network drives appropriate to the account holder's job and responsibilities.
- 1.11.4 Temporary visitors to the NDS, e.g. contractors, will not be granted access to a computer account. Physical access to the buildings and offices will only be allowed if accompanied by a member of NDS.
- 1.11.5 Full procedures for authorisation and authentication are provided in the NDS System Level Security Policy and IMSU Security Policy.

### **1.12 Building Security**

- 1.12.1 All external doors to NDS buildings will be security locked at ALL times. Internal offices must be locked independently when not in use and offices that are involved in processing sensitive data will be subject to greater security processes, which should be detailed in individual project policy.
- 1.12.2 Staff will be issued with swipe cards, key fobs and keys that are appropriate to their level of work. Staff are responsible for their swipe cards, key fobs and keys and are to notify the NDS Business Administrative Unit immediately in the event of loss. Staff must not share or give keys and swipe cards to any third parties.
- 1.12.3 The NDS Business Administrative Unit will be responsible for arranging and monitoring regular audits of door access. The results of audits will be recorded and logged. Audits will be carried out no less than quarterly.

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

### **1.13 Network and Systems IT Security**

- 1.13.1 The computer network is part of the University of Oxford network and is managed by system administrators Information Management Services Unit (IMSU). IMSU are a group of system administrators and IT support employed by and on behalf of the University Medical Sciences Division. The NDS IT Officer audits and monitors the NDS systems and has limited access to the IMSU administration systems.
- 1.13.2 Full details of the structure, operation and responsibilities for the network and computer systems are contained in the NDS System Level Security Policy.
- 1.13.3 The NDS Executive Committee will be responsible for authorising the System Level Security Policy and the IT Officer is responsible for ensuring that the systems are risk assessed, audited and tested.

### **1.14 Computers, Software and Hardware**

- 1.14.1 Control measures for NDS hardware and software are defined in the IMSU Security Policy.
- 1.14.2 All staff are expected to have read and understood the IMSU Security Policy. An electronic copy of the policy will be emailed to every new member of staff and important elements will be highlighted at the IT Induction meeting which all new staff are required to attend.
- 1.14.3 Line managers will ensure that their staff are adhering to the IMSU Security Policy. Any breaches will be reported in the first instance to the IT Officer.

### **1.15 Information Handling**

- 1.15.1 Control measures for NDS Information Handling are defined in the Information Handling Policy.
- 1.15.2 All staff are bound to the University confidentiality agreement by their employment contract. A copy of their contract will be given to staff when they commence employment. Staff are expected to comply with this agreement at ALL times.
- 1.15.3 All visitors are bound to the University confidentiality agreement by the Visitors Agreement which they must sign before coming to in the NDS. A copy of their Visitors Agreement will be given to visitors during their induction meeting. Visitors are expected to comply with this agreement at ALL times.
- 1.15.4 The confidentiality agreement is enforceable in respect of both electronic and hard copy data files. Staff and visitors are expected at ALL times to observe due diligence and care when handling and processing paper documents, computer files, electronic



The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

records, CDs, DVDs, disks drives, USB sticks or any other storage or processing medium.

- 1.15.5 All staff dealing with Personnel data are required to undertake training in relation to the Data Protection Act 1998, before access to Personnel data is authorised.
- 1.15.6 All projects will be subjected to a formal risk assessment which will include information and data handling. If appropriate to the nature of the project Information Handling SOPS will be provided and will be expected to be followed. ICT requirements to process and work on sensitive data are defined in the Information Handling policy.
- 1.15.7 All staff should keep a clear desk and clear screen when leaving the office or work station unattended. All papers should be removed from the desk and securely stored. Computer screens containing sensitive information should not be visible to others, inside or outside the premises. Screen savers must be activated and employed when the authorised user is away from the computer.
- 1.15.8 NDS provides shredders for the secure disposal of any hardcopy work that requires disposal.
- 1.15.9 Computers, mobile devices, CDs, DVDs, disk drives, USB stick or any other storage or processing medium that require disposal should be returned to the NDS IT Officer for secure disposal according to the University's policy for computer disposal:  
<http://www.ict.ox.ac.uk/oxford/disposal/>.

## **1.16 Application Development and Validation**

- 1.16.1 Any new software application should where practical be subject to validation and control. Proper risk assessment should be employed on all projects that are developing new applications.

## **1.17 Back-up and Archiving:**

- 1.17.1 All data must be archived appropriately when they are no longer required within NDS.
- 1.17.2 Hardcopy data must be recorded and moved to secure storage. The security level of archive storage must be the subject of a risk assessment which takes into account the nature of the data to be stored.
- 1.17.3 Electronic data should not be archived unless all identifiers have been removed. Identifiable data, if kept, must be encrypted. The nature and security to be used on

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

the archive data will be subject of a risk assessment and be of an appropriate level. Details of facilities for archiving are detailed in the NDS System Level Security Policy.

1.17.4 Back-up of all Electronic data is detailed in full in the NDS System Level Security Policy.

### **1.18 Projects**

1.18.1 Each project undertaken by the NDS will be subject to a full risk assessment prior to start up, and reviewed during the operation of the project and at the end of the project.

1.18.2 All NDS projects will be subject to the level of security as detailed in the NDS System Level Security Policy and the IMSU Security Policy unless it is deemed upon risk analysis that the project requires a greater level of security.

1.18.3 If any NDS project requires a separate security policy it will be deemed to be “exceptional” and provision will be made to ensure that the data is secured appropriately.

1.18.4 The Information Security Manager will be responsible for ensuring that the project specific security policy will be written, implemented, reviewed and tested.

1.18.5 NDS staff must ensure that all projects are risk assessed and any exceptional requirements are notified to the IT Officer or Information Security Manager.

### **1.19 Encryption**

1.19.1 No data of a sensitive nature and no personally identifiable data will be removed from the unit under any circumstances, unless appropriate measures, as defined in the Information Handling policy, are in place.

1.19.2 Staff wishing to take work away from NDS, for example taking results to discuss with a collaborator, will be required to store their work on a (FIPS) 256b Encrypted USB memory storage device.

1.19.3 Encryption will not be used on standard electronic storage unless a risk assessment highlights the need. If required Cryptographic controls will be compliant with the current international standards (FIPS)

### **1.20 Remote Access and Home Working**

1.20.1 Any member of staff wishing to work from home must sign and return the accessing NDS network from home form and to have understood the rules (Remote Working

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

Policy) in relation to home working. The NDS Remote Working Policy will be issued to all new staff.

- 1.20.2 NDS staff are allowed to access non-sensitive data from home using the NetStorage web access. There should be no sensitive data accessible via NetStorage web access.
- 1.20.3 When working remotely NDS staff should use the University's Virtual Private Network (VPN) service.

### **1.21 Disaster Recovery and Business Continuity**

- 1.21.1 NDS has a disaster recovery plan in place and a risk assessment is in place, which is part of the NDS Risk Register. Business continuity planning forms part of that plan. The plan will be reviewed annually.
- 1.21.2 IMSU are responsible for data backup and recovery of network drives they provide. NDS staff are informed, during the IT induction, that it is good practice to store all electronic data on network drives.
- 1.21.3 ITS provide TSM data backup and long-term archive service for the backup of university-related work. This service is available to Oxford University staff, senior members and postgraduates. Guidelines for acceptable use of HFS backup services can be found at <http://www.oucs.ox.ac.uk/hfs/policy/acceptuse.xml>.

### **1.22 Sanctions**

- 1.22.1 Suspected breaches of any part of NDS Information Security Policy and related policies should in the first instance be reported to the line manager of the staff member concerned.
- 1.22.2 All breaches and incidents should also be reported to the IT Officer and Information Security Manager. Incidents that are deemed to be serious will then be reported to the NDS Executive Committee. A log of breaches will be kept by the IT Officer. Thefts must be reported to the police and a crime number recorded. Loss of sensitive data must be reported to the University's Data Protection team (data.protection@admin.ox.ac.uk) and the Information Security Team (infosec@it.ox.ac.uk).
- 1.22.3 Any member of staff who is deemed to have deliberately or maliciously breached NDS Information Security Policy will be subject to the appropriate HR Policy sanctions.

The Nuffield Department of Surgical Sciences	Information Security Policy	NDS Information Security Policy v1.0.docx
--	-----------------------------	---

### **1.23 Risk Assessment**

1.23.1 The NDS do have an up to date Risk Register and Asset Register. All NDS projects will be required to have completed and recorded a risk assessment.

1.23.2 The NDS Executive Committee must be notified of any significant risks identified in a risk assessment and plans should be put in place for appropriate mitigation.

### **1.24 Connected Policies and References**

#### **1.24.1 University of Oxford Policies**

NDS is required to abide by any University of Oxford IT and Information Security Policies that are in place. Current policies will be detailed in full on the [www.ox.ac.uk](http://www.ox.ac.uk) website.

#### **1.24.2 IMSU Policies**

IMSU have an additional set of Policies and SOP's that NDS must conform to. The current policies are detailed on [www.imsu.ox.ac.uk](http://www.imsu.ox.ac.uk).

#### **1.24.3 NDS Policies**

This information security policy is designed to be read in conjunction with all other current NDS policies relating to IT and information handling. A full list is referred to in Annex B.

## 1.25 Annex A

---

### 1.25.1 Regulation and Governance:

This policy was written with Reference to the following:

The Computer Misuse Act (1990)

The Data Protection Act (1998)

The Regulation of Investigatory Powers Act (2000)

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)

The Freedom of Information Act (2000),

ISO/IEC : 27001

ISO/IEC: 27002

ISO/IEC: 27005 (BSI 7799-3)

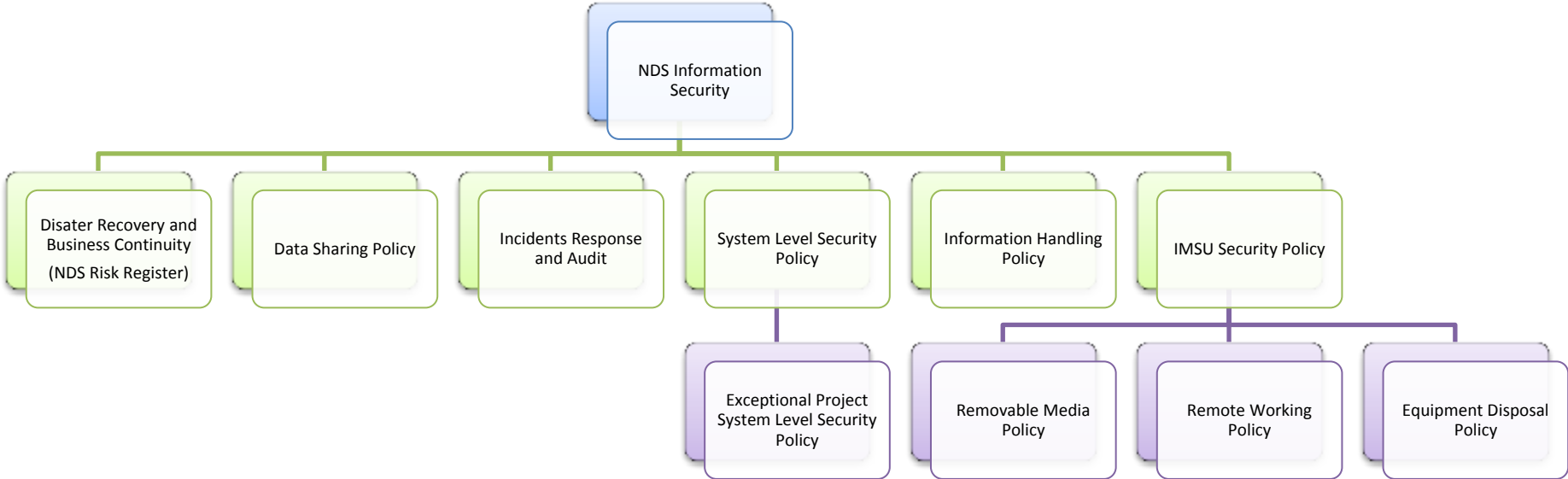
BSI 25999

ISO 15489

NIST FIPS PUB -46-3, 140-2, 180-3, 186-3 & 197

# 1.26 Annex B

## 1.26.1 NDS IT and Information Security Policies:



Sops and Guidance Documents

Risk Register and Risk Assessments

Asset Register