THE JENNER INSTITUTE
DEVELOPING INNOVATIVE VACCINES

UNIVERSITY OF OXFORD

Information Security Policy

Effective date:
Version: **2014v1**

Author	Name: Gary Srickland	Title: Business Manager.
	Signature: GSRickland	Date: 12/6/14.
Reviewed by	Name: Andrew Allen	Title: IT Manager
	Signature: DJAllen	Date: 12/6/14
Authorised by	Name: Adrian Hill	Title: Director
	Signature: AVHill	Date: 12/6/14

1.1 Introduction

1.1.1 This policy is designed to be the overarching Information Security Policy for the Jenner Institute and is the primary policy under which all other technical and security policies reside.

1.1.2 The policy is designed to ensure that the Jenner Institute will comply with all relevant compliance legislation in respect of information security. The policy will describe specific Jenner Institute 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 Jenner Institute 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 Jenner Institute 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, students and academic visitors to the Jenner Institute.

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 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 (http://www.admin.ox.ac.uk/ictc/)
IT	Information Technology
ITS	Oxford University's IT Services (http://www.it.ox.ac.uk/)
MSD	Medical Sciences Division
MSD IT SERVICE	Information Management Services (http://www.MSD IT Service.ox.ac.uk/)
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 Director of the Jenner Institute.

1.6.2 The Information Security Officer for the Jenner Institute is ***Gary Strickland.***

1.6.3 The Jenner Institute Management Committee is the designated owner of the Information Security Policy.

1.6.4 The IT Manager for the Jenner Institute is ***Andrew Allen.***

1.6.5 The Data Controller for the Jenner Institute is the named University of Oxford Data Controller.

1.6.6 Oxford University 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 Jenner Institute 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 Officer 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.

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 Officer 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 once a year. This frequency will be reviewed if neccercery.

1.8.2 The Information Security Policy will be reviewed annually by the Information Security Officer and approved by the Jenner Institute Management 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 MSD IT Services. MSD IT SERVICE's network infrastructure connects the Jenner Institute to the University's network.

1.10.2 All users of the Jenner Institute 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 Jenner Institute 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 will be given IT induction before being allowed access to University network. This will cover all aspects of the Institute Information Security Policy.

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

amendments) and available 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 Manager.

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 Manager.

1.11 Authentication and Authorisation

1.11.1 All members of staff will be issued with a University Card. This card will give the Jenner Institute the authority for the member to become a user of the MSD IT SERVICE 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 are set up with a computer account subject to line manager approval. Application will be made by the Jenner Institute and is processed by the MSD IT SERVICE 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 Jenner Institute, 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 Jenner Institute.

1.12 Building Security

1.12.1 All external doors to Jenner Institute locations 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.

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 Jenner Institute 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 Jenner Institute 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.

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 (MSD IT SERVICE).

MSD IT SERVICE are a group of system administrators and IT support employed by and on behalf of the University Medical Sciences Division. The Jenner Institute IT Manager audits and monitors the Jenner Institute systems and has limited access to the MSD IT SERVICE administration systems.

1.13.2 The structure, operation and responsibilities for the network drives and computer systems are managed in the Jenner Institute by the IT Manager.

1.14 Information Handling

1.14.1 Control measures for Jenner Institute Information Handling are delegated to the Business Manager.

1.14.2 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.

1.14.3 All visitors are bound to the University confidentiality agreement by the Visitors Agreement which they must sign before coming to in the Jenner Institute. 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.

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

1.14.5 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.

1.14.6 Where appropriate, critical projects will be subjected to a formal risk assessment which will include information and data handling.

1.14.7 Computer screens containing sensitive information should not visible to others, inside or outside the premises. Screen savers must be activated and employed when the authorised user is away from the computer.

1.14.8 The Jenner Institute provides shredders for the secure disposal of any hardcopy work that requires disposal.

1.14.9 Computers, mobile devices, CDs, DVDs, disk drives, USB stick or any other storage or processing medium that require disposal should be returned to the Jenner Institute IT Manager for secure disposal according to the University's policy for computer disposal: http://www.ict.ox.ac.uk/oxford/disposal/.

1.15 Application Development and Validation

1.15.1 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.

1.16 Back-up and Archiving:

1.16.1 All data must be archived appropriately when they are no longer required within Jenner Institute.

1.16.2 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 Encryption

1.17.1 No data of a sensitive nature and no personally identifiable data will be removed from the unit under any circumstances, unless discussed with the Jenner Institute's Information Security Officer.

1.17.2 Staff wishing to take work away from the Jenner Institute, 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.

1.17.3 Encryption will not be used on standard electronic storage unless a risk assessment highlights the need.

1.18 Remote Access and Home Working

1.18.1 Any member of staff wishing to work from home must sign and return the accessing Jenner Institute network from home form and to have understood the rules (Remote Working guidelines) in relation to home working.

1.18.2 When working remotely Jenner Institute staff are required to use the University's Virtual Private Network (VPN) Cisco service. This service can be downloaded form the webauth pages found here: https://register.ox.ac.uk

1.19 Disaster Recovery and Business Continuity

1.19.1 The Jenner Institute (ORCRB) has a disaster recovery plan in place and a risk assessment is in place, which is part of the Jenner Institute Risk Register. Business continuity planning forms part of that plan. The plan will be reviewed annually.

1.19.2 MSD IT SERVICE are responsible for data backup and recovery of network drives they provide. Jenner Institute staff are informed, during the IT induction, that it is good practice to store all electronic data on network drives.

1.19.3 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.

1.20 Sanctions

1.20.1 Suspected breaches of any part of Jenner Institute Information Security Policy and related policies should in the first instance be reported to the line manager of the staff member concerned.

1.20.2 All breaches and incidents should also be reported to the IT Manager and Information Security Officer. Incidents that are deemed to be serious will then be reported to the Jenner Institute Management Committee. A log of breaches will be kept by the IT Manager. 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).

1.20.3 Any member of staff who is deemed to have deliberately or maliciously breached Jenner Institute Information Security Policy will be subject to the appropriate HR Policy sanctions.

1.21 Risk Assessment

1.21.1 The Jenner Institute has an up to date Risk Register and Asset Register.

1.21.2 The Jenner Institute Committee must be notified of any significant risks identified in a risk assessment and plans should be put in place for appropriate mitigation.

1.22 Connected Policies and References

1.22.1 **University of Oxford Policies**

Jenner Institute 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 website.

1.22.2 **MSD IT SERVICE Policies**

MSD IT SERVICE have an additional set of Policies and SOP's that Jenner Institute must conform to. The current policies are detailed on www.MSD IT Service.ox.ac.uk.

1.23 Annex A

1.23.1 **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