MAC MANAGED PLATFORM
SERVICE LEVEL AGREEMENT

Oxford University Computing Services
Network Systems Management Service

Version: 1.0
Release Date: 09/05/2011
Document Control

Authors
Wylie Horn, Jon Hutchings, Marko Jung, James Partridge, and Marcus Saunders

Document Storage
The document is located at http://www.oucs.ox.ac.uk/nsms/slas/

Document Approval
This document has been approved for use by:

- NSMS Section Manager
- NSMS Deputy Section Manager
- NSMS Mac Support Team

Distribution List
The following parties will be informed by email when an updated copy of the service level agreement (SLA) is uploaded to the NSMS web site:

- Client’s administrative contacts
- Client’s technical contacts
- NSMS Section Manager
- NSMS Deputy Section Manager
- NSMS Mac support team

Amendment History
09/05/2011 Version 1.0
# Table of Contents

1 Introduction 5  
2 Scope 6  
3 Exceptions 7  
4 Key Contacts 8  
5 Service Level Agreement Management 9  
5.1 Service Level Agreement Administration 9  
5.2 Service Level Agreement Change Management 9  
5.3 Force Majeure 9  
5.4 Performance Reporting and Inventory 9  
6 Service Components 10  
6.1 Central MMP Infrastructure 10  
6.2 Operating System Installation, Patches and Upgrades 10  
6.3 Application Software Installation, Patches and Upgrades 11  
6.4 Centralised System Configuration 11  
6.5 Security 11  
6.6 Backup 13  
6.7 Hardware 13  
6.8 User Support (Help Desk) 14  
7 Service Provision Schedule 16  
7.1 General Service availability 16  
7.2 Central MMP Infrastructure Schedule 16  
7.3 Operating System and Application Software Schedule 16  
7.4 Backup Schedule 17  
7.5 User Support Schedule 18  
Appendix A Supplemental Material 21  
A.1 MMP Documentation 21  
A.2 NSMS Services and Service Level Definitions 21  
A.3 OUCS Service Level Definitions 21
## Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMP</td>
<td>Managed Mac Platform</td>
</tr>
<tr>
<td>OS X</td>
<td>Apple's operating system for computers</td>
</tr>
<tr>
<td>iOS</td>
<td>Apple's operating system for mobile devices (iPhone, iPad, iPod)</td>
</tr>
<tr>
<td>NSMS</td>
<td>Network System Management Service</td>
</tr>
<tr>
<td>OUCS</td>
<td>Oxford University Computing Service</td>
</tr>
<tr>
<td>ITSS</td>
<td>IT Support Staff</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

The NSMS group provides a Managed Mac Platform (MMP) service to colleges and departments. The aim of the service is to provide users of the service with a highly integrated, reliable and resilient desktop environment to support research and administrative tasks.

1.1 Purpose

This document describes the parameters of the service. The document will be reviewed annually in the light of experience gained managing the service, and any necessary changes will be made with the agreement of both parties.
2 Scope

This service level agreement covers the delivery and support of the following services:

- Apple Mac Workstation hardware
  - Supported Apple Mac hardware
  - Supported peripherals and printers
- Apple Mac workstation software
  - Operating system deployment and updating
  - Standard software package deployment and updating
  - Special purpose software
  - Software licensing
- Data backup
- System security
- Support
- Change management
- Service infrastructure
3 Exceptions

The following are omitted from the SLA:

- Hardware
  - Systems not owned by the University of Oxford
  - iOS devices (i.e. Apple iPhone, Apple iPad, Apple TV)
  - Unsupported or non-standard hardware or peripherals (i.e. anything not in the supplemental MMP hardware compatibility lists)

- Software
  - Unsupported or non-standard software (i.e. anything not in the supplemental MMP software compatibility lists)
  - Assistance with specialist software (i.e. advice about or tuition in how to use a specialist application)

- Office peripherals (e.g. Fax machines, photocopiers, all-in-one devices, telephones)

- Audio-visual equipment (e.g. televisions, video systems, DVD recorders)
4 Key Contacts

4.1 NSMS Support
All support and change requests should be sent to the NSMS Mac Team
email: nsms-mac@oucs.ox.ac.uk    phone: +44 (0)1865 273 209

4.2 Departmental Consultation
The client will provide contact details for at least one technical contact and one administrative contact.

4.3 NSMS Management
These contacts are given for information and escalation purposes only.
Wylie Horn - NSMS Section Manager
email: wylie.horn@oucs.ox.ac.uk    phone: +44 (0)1865 283 410

Jon Hutchings - NSMS Deputy Section Manager
email: jon.hutchings@oucs.ox.ac.uk    phone: +44 (0)1854 283 290
5 Service Level Agreement Management

5.1 Service Level Agreement Administration
Updates to the service level agreement are the responsibility of the NSMS Section Manager and NSMS Mac Team.

5.2 Service Level Agreement Change Management
NSMS and clients of the service will review this service level agreement annually in Hilary term. We are not adopting a formal change management process. Any agreed changes will be implemented in Trinity term of the same year.

5.3 Force Majeure
Either NSMS or the client may suspend the SLA on request in the event of a catastrophic event or any other event deemed critical enough to warrant the suspension of the SLA. Suspension of the SLA will only occur with the agreement of both parties.

5.4 Performance Reporting and Inventory
Clients may request inventory reports for Macs managed by the service.
6 Service Components

6.1 Central MMP Infrastructure

The MMP relies on infrastructure hosted and maintained by NSMS. It is the client’s responsibility to ensure that their network infrastructure provides the necessary means for MMP workstations to access the NSMS management infrastructure. NSMS will liaise with the OUCS Networks group to ensure that service delivery is adequate from OUCS to a unit’s FroDo switch.

NSMS will provide documentation containing all administrative and technical details necessary for the successful operation of the service (see Appendix A.1). NSMS can also offer an embedded Linux system that monitors the ability of Managed Macs to contact the central MMP infrastructure.

6.2 System requirements

Infrastructure

- At least 100MBit/sec Ethernet or OWL phase 2 WiFi with private SSID
- DHCP
- Addition of the NSMS NetBoot server as ip-helper-address
- Firewall modifications to allow access from and to central MMP infrastructure
- Clients with more than 50 users are asked to provide a SMB or AFP network volume with about 300GB for software package deployment.

Minimum hardware spec

- Mac computer with an Intel processor
- Minimum of 1GB RAM, preferably ≥ 2GB
- Minimum 64GB storage

Other

- Clients are required to provide electronic copies of invoices for new hardware and software licenses

6.3 Operating System Installation, Patches and Upgrades

NSMS generally installs managed Mac desktops and laptops with the latest major release of OS X. Operating System and software installation takes place via an MMP workstation’s wired network connection. NSMS will test security patches and minor version operating system updates, and these will be deployed automatically to all workstations using a central software update service according to the schedule defined in Section 7.3.

NSMS installs the same major version of OS X on all of a client’s managed hosts. After the release of a new major version of Apple Mac OS X, NSMS will assist the client in developing a migration strategy but will continue to support the
previous release for a minimum of 1 year. Extended support beyond this period is available as a premium service.

It is the client’s responsibility to purchase all operating system licences and to provide proof of purchase to NSMS. All purchase information will be added to our inventory database. On request, NSMS will provide a report detailing purchase information.

**6.4 Application Software Installation, Patches and Upgrades**

NSMS deploys a standard suite of site-licensed software to all managed hosts. A list of available applications can be found in the software compatibility list at the NSMS web site (as detailed in Appendix A.1). NSMS offers the installation of additional software packages as detailed in the software compatibility list. The deployment and maintenance of certain complex software packages may involve an additional charge.

NSMS generally supports the deployment of the latest and previous major versions of a software product. More complex or frequently updated software may be excluded from this deployment strategy. Details are outlined in the software compatibility list.

Support for an earlier version of an application will be discontinued once the new major version of an application is released to the MMP. NSMS will assist the client in developing a migration strategy. Extended support for legacy software versions is available as a premium service.

A selection of free software and freeware applications is offered by NSMS on a "best efforts" basis through a self-service portal. Support for software provided by the self-service portal may be discontinued without further notice.

It is the client’s responsibility to acquire all additional software licenses before deployment, and to provide NSMS with electronic proof of purchase. On request, NSMS will provide a software inventory report and purchasing information.

**6.5 Centralised System Configuration**

All client machines are deployed with a core set of system settings intended to assist the client in bringing the workstation in alignment with University IT regulations. Additional settings (including branding) may be defined by the unit in consultation with NSMS as outlined in Appendix B.

**6.6 Security**

NSMS’s security responsibilities are limited to authentication, patching, anti-virus measures, and compliance tests.
6.6.1 Authentication and Authorisation

NSMS will be responsible for any server based authentication and authorisation mechanisms the service uses. Integration into other existing directory services may be considered for larger deployments as a premium service.

NSMS will have the sole administrative account on managed machines. Attempts to circumvent this will invalidate the terms of the MMP service.

Users will be provided with a standard non-administrative user account (a standard user account).

6.6.2 Anti-virus

NSMS deploys the University of Oxford's site-licensed anti-virus package to all managed hosts. Virus definitions will be updated automatically as they become available. The software will be installed and configured to comply with agreed licensing conditions.

Although the site-licensed anti-virus package will be deployed by NSMS, it remains the client’s responsibility to ensure that all managed hosts connect regularly to the virus definition update servers.

6.6.3 Patching

NSMS monitors the patch status of all managed workstations to ensure they are patched appropriately.

In the event that a managed workstation misses four consecutive scheduled updates, as described in Section 7.3, NSMS reserves the right to exclude this workstation from the MMP service until all available updates and patches are applied.

6.6.4 Compliance

The client is responsible for compliance with the following UK legislation (in regard to IT):

• Data Protection Act (1998)

The client is responsible for compliance with the following University regulations (in regard to IT):

• Oxford University Acceptable Use Policy¹

6.7 Virtualisation

NSMS can provide virtualisation software that allows "guest" operating

¹ http://www.ict.ox.ac.uk/oxford/rules/
systems such as Windows or Linux to run on MMP machines, subject to the following conditions:

Purchase of the appropriate guest operating system licence is the responsibility of the client.

Management of a virtual machine is entirely the responsibility of the client; guest operating systems are not covered under the terms of the MMP.

A client using a virtual machine agrees to maintain the guest operating system software, keeping it up to date and secure against intrusion by installing the University site-licensed antivirus software. Guest operating systems must be compliant with University IT policy.

Backup of the virtual machines will be the responsibility of the client.

6.8 Backup
NSMS will deploy the University of Oxford’s site-licensed backup client software. This software will allow workstations to be backed up on a scheduled basis using the University’s central backup service. NSMS takes no responsibility for failed, incomplete or missed backups caused by circumstances other than the installation and configuration of the backup client software.

Additional backup arrangements to augment this service will be the responsibility of the client.

6.9 Hardware

6.9.1 Hardware lifecycle management
The MMP does not include hardware (or peripheral) lifecycle management. The client is responsible for purchasing, repairs, and disposal of equipment. All new Apple Mac desktops and laptops should be purchased with a 3-year warranty (available at no additional cost from Apple Higher Education). NSMS recommends that the participating unit replaces systems on a 4 year replacement cycle or upon warranty expiry. NSMS reserves the right to exclude out of warranty workstations from the MMP.

NSMS can purchase hardware on behalf of a client through its centralised purchasing service. Details and procedures can be found at the NSMS web site (see Appendix A.2).

6.9.2 Evaluation of new Apple hardware
NSMS will keep abreast of Apple’s hardware replacement cycle and base the service on appropriately specified desktop and laptop machines.

NSMS offers advice on hardware specifications prior to rollout to ensure the client’s requirements are met.
6.9.3 Printers

The configuration of printers on managed Macs is limited to networked workgroup printers where either Apple provides a PPD or the printer manufacturer provides a compatible printer driver.

NSMS deploys up to ten printer configurations per unit. NSMS will charge for any work resultant from setting up additional or specialist printers.

It is the client’s responsibility to ensure purchased printers are compatible with the release of Apple Mac OS X in use. The client may consult NSMS prior to purchasing printer hardware to ensure the requirements are met.

6.9.4 Other peripherals

Setup and configuration of any other peripheral devices is chargeable at standard NSMS rates.

6.9.5 Health and Safety – PAT, DSE assessment

It is the client’s responsibility to ensure compliance with health and safety regulations including PAT and DSE assessments.

6.10 User Support

As with many services provided by OUCS, support is provided through a combination of OUCS and local IT Support Staff (ITSS). Users may always contact NSMS (the Managed Mac Platform provider) regarding any aspect of the service.

Primary support is generally provided either by local ITSS or by NSMS:

i. Local ITSS as the primary support path:

In cases where primary support is provided by local ITSS, users should always contact their local ITSS with any support issues in the first instance. If local ITSS are unable to resolve a support request directly they will refer the issue on behalf of the user to NSMS. Where necessary, NSMS will seek the approval of the unit’s administrative contact to approve any chargeable support work where such work falls outside the scope of the SLA.

ii. No Local ITSS:

If there are no local ITSS, or NSMS themselves are acting in this capacity, users may contact NSMS directly using the NSMS RT (job tracking) system as stated in section 4.1 above. Where necessary, NSMS will seek the approval of the unit’s administrative contact to approve chargeable support work where such work falls outside the scope of the SLA.

The NSMS group will support the service using the following means:

• Platform support:
  NSMS supports the deployment and centralised configuration of the
operating system and selected application software as defined in the MMP compatibility lists. The service does not include a formal Help Desk for end user support regarding application usage, software issues, peripherals or user-induced problems.

- **Infrastructure support:**
  NSMS will support the server infrastructure on which the service relies.

- **External Referral:**
  If necessary the NSMS group will liaise with external software and hardware suppliers to resolve any problems.

- **Escalation:**
  NSMS will provide escalation procedures to ensure that client queries are dealt with satisfactorily. These are described in Section 7.5.2 below.

It is the client’s responsibility to report all incidents as well as requests for service modifications or new aspects of the service to NSMS.
7 Service Provision Schedule

7.1 General Service availability

7.1.1 Hours of Service

The Managed Mac Platform operates at all times.

NSMS staff cover is available from 0900 to 1700 on weekdays (excluding public holidays and annual OUCS closures). Automatic monitoring of the service takes place outside these hours. NSMS staff will be notified of any issues and will respond to them on the following working day.

7.1.2 Resilience

The core infrastructure of the Managed Mac Platform, such as servers and storage, have been deployed with resilience and business continuity in mind.

The central infrastructure hardware is located in the OUCS data centre. Complete failure of this site would result a total loss of the central management facilities, directory service, and file services. Offsite backup of servers is managed using the OUCS HFS data service as outlined in section 7.4 below.

NSMS continuously reviews its disaster recovery strategies in accordance with the general OUCS strategy.

7.2 Central MMP Infrastructure Schedule

NSMS will be solely responsible for the operation, maintenance, and backup of the infrastructure that delivers the Managed Mac Platform to users.

NSMS will ensure that this hardware and software meets the operational requirements of the service and will be responsible for any hardware or software upgrades required to ensure the on-going operation of the service.

Software updates are provided by the relevant software vendor and applied by NSMS. Except in the case of emergency maintenance (e.g. security fixes), clients will be notified of any scheduled downtime at least two days in advance.

If NSMS is notified of a fault on the MMP central infrastructure between 0900 and 1700 on a working day, NSMS will commence investigation within one hour (provided that no similar fault is also being handled by the same team). If a fault occurs outside these hours NSMS will respond on the following working day.

7.3 Operating System and Application Software Schedule

NSMS will be solely responsible for the installation and management of software on managed Mac desktops and laptops.
The network-based operating system installation for registered workstations can be invoked by local ITSS or the user. This process re-installs the operating system thereby erasing all data on the system volume 'Macintosh HD'. Afterwards the deployment mechanism updates the system to the latest expected state, including application software.

Each unit has a defined weekly two hour 'at risk' period for all managed Mac workstations either in the morning (1100-1300) or afternoon (1400-1600). NSMS generally deploys software updates to the operating system and all supported software applications during this period. Critical security patches may be deployed at any time.

NSMS will inform the user when performing software installations, patches, or system updates using system notifications. The user will be asked to log out or restart when necessary. It is the client's responsibility to perform those actions when indicated.

A client may opt individual workstations out of an update cycle for up to four weeks using the standard support path as described in Section 7.5. However, if opting back in to the scheduled update cycle causes significant extra work NSMS reserves the right to charge for this service.

### 7.4 Backup Schedule

As outlined in section 6.8, the NSMS team will deploy the University of Oxford’s site-licensed backup client software. Details of the client data retention policy are available in Section 3.5 of the *HFS Further Information* document\(^2\). The volume labelled *Macintosh HD* will be excluded from all backups; user data stored on the *LocalStorage* volume will be backed up as normal.

The servers upon which the MMP service relies are backed up on a scheduled basis using the OUCS enterprise backup systems. The data will be backed up on a 90 day / 90 copy rotation.

Users may also make local backups on their own removable media. Backing up using Apple's Time Machine utility is not supported by NSMS.

\(^2\) [http://www.oucs.ox.ac.uk/hfs/help/furtherinfo.xml](http://www.oucs.ox.ac.uk/hfs/help/furtherinfo.xml)
### 7.5 User Support Schedule

Support requests should be submitted by e-mail to the NSMS RT ticketing system at nsms-mac@oucs.ox.ac.uk. Users will receive an autoreply with a ticket number which should be included in all related correspondence.

Urgent support requests (priority levels 1 and 2 in the table below) can be made by telephone to +44 (0)1865 273 209.

User support is provided between 0900 and 1700 on weekdays (excluding public holidays and annual OUCS closures). NSMS staff will respond to user support requests generated outside these hours on the following working day.

#### 7.5.1 Service Levels

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Description</th>
<th>Target response time</th>
<th>Target time to initiate diagnosis</th>
<th>Target fix/work around time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System failure³: <em>user unable to work</em></td>
<td>1 hour</td>
<td>2 hours</td>
<td>4 hours</td>
</tr>
<tr>
<td>2</td>
<td>Software problem: <em>user unable to perform some key tasks</em></td>
<td>2 hours</td>
<td>4 day</td>
<td>2 days</td>
</tr>
<tr>
<td>3</td>
<td>Intermittent hardware or software problem: <em>user still able to perform key tasks</em></td>
<td>4 hours</td>
<td>2 days</td>
<td>5 days</td>
</tr>
<tr>
<td>4</td>
<td>Information request only: <em>no immediate problem.</em></td>
<td>4 hours</td>
<td>2 days to provide initial update</td>
<td>10 days to provide information/advice</td>
</tr>
</tbody>
</table>

Table 1 NSMS MMP Service Levels

Service levels only apply to the previously described core working hours and Mac Managed Platform support.

---

³ If the system would require extensive maintenance to return it to a fully working state NSMS reserve the right to rebuild the system rather than to repair it.
7.5.2 Escalation Routes

If service levels are not met then the following escalation processes should be followed.

<table>
<thead>
<tr>
<th>Reason for Escalation</th>
<th>Escalation Level First</th>
<th>Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support request not assigned under the terms of the SLA</td>
<td>NSMS Mac Support Team</td>
<td>NSMS Section Manager</td>
</tr>
<tr>
<td>Support request not responded to under the terms of the SLA</td>
<td>NSMS Mac Support Team</td>
<td>NSMS Section Manager</td>
</tr>
<tr>
<td>Support request left unresolved under the terms of the SLA</td>
<td>NSMS Mac Support Team</td>
<td>NSMS Section Manager</td>
</tr>
<tr>
<td>User complaint</td>
<td>NSMS Section Manager</td>
<td>OUCS Director</td>
</tr>
<tr>
<td>Unacceptable User behaviour</td>
<td>Head of Department/College Bursar</td>
<td>University Personnel</td>
</tr>
<tr>
<td>Workaround solution not accepted by the user</td>
<td>NSMS Section Manager</td>
<td>OUCS Director</td>
</tr>
</tbody>
</table>

Table 2 NSMS MMP Escalation Procedures
8 Termination of Service

When an MMP Mac is decommissioned NSMS undertake to complete the following:

1. All user data on an MMP workstation will be retained.
2. Macintosh HD will be securely wiped; the latest licensed version of Mac OS X will be installed and the primary user account recreated.
3. The Mac will be deregistered from HFS and removed from the NSMS management infrastructure.
4. On request, local ITSS will be provided with details of the MMP partition scheme, which they can continue using or reconfigure as required.

At the unit’s request a decommissioned MMP workstation can be returned in a different state from that described above. However, any work over and above the standard decommissioning procedure will be charged at the standard NSMS hourly rate.
APPENDIX A SUPPLEMENTAL MATERIAL

A.1 MMP Documentation
Mac Managed Platform pricing
http://www.oucs.ox.ac.uk/nsms/services/mmp.xml
Mac Managed Platform software compatibility list
http://www.oucs.ox.ac.uk/nsms/services/mmp/software_compatibility.xml
Mac Managed Platform hardware compatibility list
http://www.oucs.ox.ac.uk/nsms/services/mmp/hardwareCompatibility.xml
Mac Managed Platform infrastructure requirements
http://www.oucs.ox.ac.uk/nsms/services/mmp/infrastructure.xml

A.2 NSMS Services and Service Level Agreements
NSMS Centralised Purchasing Service
http://www.oucs.ox.ac.uk/nsms/services/purchasing.xml
NSMS Hourly Charged Services
http://www.oucs.ox.ac.uk/nsms/charges/costs.xml.ID=hourly-charges

A.3 OUCS Service Level Agreements
OUCS General SLD
http://www.oucs.ox.ac.uk/internal/sld/oucs.xml
OUCS Dynamic Host Configuration Protocol (DHCP) SLD
http://www.oucs.ox.ac.uk/internal/sld/dhcp.xml
OUCS Hierarchical File Server (HFS) SLD
http://www.oucs.ox.ac.uk/internal/sld/hfs.xml
OUCS Antivirus SLD
http://www.oucs.ox.ac.uk/internal/sld/antivirus.xml
OUCS Software License Administration SLD
http://www.oucs.ox.ac.uk/internal/sld/licence.xml
APPENDIX B SYSTEM CONFIGURATION

B.1 Workstations

All MMP workstations come with two partitions: Macintosh HD, for the OS and related files, andLocalStorage for all user data. This scheme separates user data from the operating system so that in the event of a serious problem the machine can be rebuilt quickly and simply without affecting user data.

All user accounts have standard user rights and privileges; admin access to an MMP machine is not granted either to users or local IT staff.

All MMP machines are deployed with a hidden (administrative) user account. This account is for use by NSMS only and the credentials will not be given to any departmental staff under any circumstances.

All MMP machines are deployed with a standard suite of site-licensed software to all managed workstations. See section 6.4 above for details.

Apple software updates and third-party application updates are deployed automatically by NSMS as outlined in section 7.3 above. Users will be notified of any updates when they occur.

All MMP workstations come with an Oxford University branded desktop.

The use of MMP workstations falls under the Regulations relating to the use of Information Technology Facilities: http://www.ict.ox.ac.uk/oxford/rules/ and users must remain in compliance with the appropriate legislation as described in section 6.6.4 above.

B.2 Requesting Changes

Requests for changes to the MMP configuration should be submitted by e-mail to the NSMS RT ticketing system at nsms-mac@oucs.ox.ac.uk. Users will receive an autoreply with a ticket number, which should be included in all related correspondence.

These changes could include deploying a specifically branded desktop image, requests for changes in update schedules, or requests for additional software. Fundamental changes to the MMP system configuration (such as granting users administrative access) cannot be accommodated.