The following Terms of Service apply to the HMS Endpoint Services Program provided by LANDesk and Casper. Other services offered by HMS IT may have their own Terms of Service.

What are Endpoints?

- **Endpoints** are devices such as desktop computers, laptops, computers, tablets, smartphones, even printers, that connect to the HMS network, and are used to perform work related to the mission of HMS.
- **Endpoint services** are a set of applications and web services implemented by HMS IT to increase information security, reduce risk of data loss and enhance support services provided by HMS IT.
- **Endpoint services** are provided by two applications: LANDesk (for Windows computers) and Casper (for Macintosh computers). We currently do not offer Endpoint Services software for Linux computers.
- **The Endpoint Services Program** operates by installing an application on the computer, gathering information about the computer hardware and applications, and then transmitting the information to the management server. The application communicates securely with a local server where data is stored. There is no external access to the server where data is stored. Please see the Collection of Information section of this document for details about what information is collected.
- **The Endpoint Services Program** software application provides a Software Self Service portal on the computer, allowing users to perform certain tasks and/or install certain software without the assistance of a Client Services Representative or the IT Service Desk.

General Description of Services

**Inventory and Asset Management Service**
Inventory & Asset Management Service offers automated inventory data collection and asset management for devices supported by HMS IT.

**Software Self Service Portal**
Software Self Service portal offers an application on the computer that can be used to install commonly requested software and request services.

**Application Deployment Service**
Application Deployment Service provides a mechanism for IT staff to deploy applications upon request by a client.

**Patch Management Service**
Patch Management Service offers OS and application patch management to computers.

**Remote Desktop Service**
Remote Desktop Service offers remote assistance from HMS IT to users’ devices.

**System Imaging Service**

Questions? Call the IT Service Desk at 617-432-2000 or visit the [HMS IT Web Site](#).
HMS IT Endpoint Services Program Terms of Service

1. The System Imaging Service allows for deployment of system restore images to computers that are brand-new or being rebuilt.

Mobile Devices
2. HMS IT is not currently requiring mobile devices such as personally owned smart phones, smart watches, and tablets to be enrolled in the HMS Endpoint Services Program.
3. Mobile devices purchased with Harvard funds are eligible to opt-in to the HMS Endpoint Services Program. Please speak with your Client Services Representative for more information.

Important Note!
Some hospitals have higher security standards, and therefore may have a higher priority over some HMS services. These devices must be handled on a case-by-case basis.

Security
The Endpoint Services Program has multiple levels of security.

IT Staff Access
- Access to the service is limited by “Need to know”. Only HMS/HSDM IT staff who need access to the service are granted access.
- IT Staff are restricted to accessing only those devices they support or need to access to perform their daily duties.
- No one outside of HMS/HSDM IT will be granted access, except as authorized by an IT Director or CIO.
- Only active IT Staff members in good standing are granted access.

Console Access
Console access is limited by “need to know”, and restricted to only those functions needed to provide support.

Transmission of Data
All data is transmitted to the server via Secure Sockets Layer (HTTPS/SSL).

Storage of Data
All data is stored in a secure database hosted by HMS in a local secure data center. Access to the database is limited to the server administrators and the database administrators.

Administrative Access to Devices
Users will retain existing levels of access to devices. For example, if you currently have administrative access to your computer, you will retain that access. If you do not have administrative access to your computer, then the access will not change.

Cyber Essentials Security Policy

Questions? Call the IT Service Desk at 617-432-2000 or visit the HMS IT Web Site.
HMS IT Endpoint Services Program Terms of Service

- The Harvard Medical School Cyber Essentials Security Policy states that all computers connecting to a non-public HMS network must be secured by systems management software, antivirus software and backup software.
- Computers which are supported by HMS IT but are located Off Quad are required to be enrolled.
- Computer whose function or age prevent the use of LANDesk or Casper but be secured using other methods.

6. Deployment methods

- Self-enroll- Any user who prefers to enroll in the Program themselves may do so by installing the software through a self service website, or contacting their department Client Services Representative or the HMS IT Service Desk.
  - Certain HMS Site license software (i.e. Adobe Acrobat Pro HMS Site License) may require enrollment in the Endpoint Services Program before the software can be installed. This requirement will be noted for any software that requires enrollment.
  - TechRefresh- All new computers and any computer imaged with the TechRefresh Deployment image will be automatically enrolled.
  - Service visits- A Client Services Representative (CSR) may enroll the computer during a service visit.
  - Department rollouts- Deployment to departments requires approval from at least the Department Administrator.
  - For basic science research departments, the department must determine the appropriate level of approval prior to deployment by IT, as individual labs may require independent approval prior to rollout.

Devices Eligible for enrollment

- All On-Quad computers connected to the HMS network are automatically eligible for these services.

  Exceptions: Certain computers will not be eligible for these services:
  - Instrument computers that would be substantially impacted by the use of the software.
  - Computers too old to run the application(s) required by the service.
  - Computers that are taken to a non-HMS supported facility (i.e., hospital) and/or have no expectation of support are considered unsupported by HMS IT and are therefore ineligible for these services.
  - HMS considers all retired computers to be no longer supported. They do not qualify for HMS sponsored software and are exempt from endpoint services tools installation.
  - Computers that are owned and/or supported by HMS but require encryption due to hospital affiliation.
  - Only computers are eligible for enrollment.
  - Personally owned mobile devices running iOS, Android, Windows Phone etc. are not eligible.
  - Institutionally owned mobile devices are eligible for enrollment, but are not required to be enrolled at this time.
  - Some tablet computers can run the Windows OS as a normal operating system. These devices are eligible for and supported by the Endpoint Services Program.
Cost

• The HMS Endpoint Services Program is provided at no cost to the user, lab, or department.
• Certain applications provided through the Self-Service Portal may have a cost associated with them. The cost will be noted in the description of the software.
• HMS can only accept a Harvard 33-digit billing code for these applications.

System Requirements

• Participation in the HMS Endpoint Services Program requires the installation of certain applications.
• To install the application the computer must meet the following requirements:
  • Windows:
    o Windows XP or later
    o At least 2 GB of RAM
    o At least 10 GB of hard disk space.
    o Wired or wireless network connection
  • Mac OS X:
    o Mac OS X 10.7 or later.
    o At least 2 GB of RAM
    o At least 10 GB of hard disk space.
    o Wired or wireless network connection

When a Device is Retired from Active Service

When a device is retired from service and is no longer supported by HMS, the inventory information will be archived, all HMS licensed software should be removed, and all management software should be removed.
When an End User Leaves HMS

• Hardware information will be retained. Software application licenses provided by HMS will be revoked. Software application licenses paid for with a 33 digit Harvard billing code and assigned to the user will be revoked and reassigned to another user within the department at the departments discretion. Software purchased by the user with the personal funds are not managed by these services, and remain the property of the user.
• To have the application software removed, contact your local Client Service Representative or the HMS IT Service Desk prior to your last day on campus. This ensures that the server will no longer try to connect to the computer, and will archive the previous data.

Changes to the Terms of Service

• The service owner and the Director of Client Services must approve policy changes.
• The HMS IT Change Management Approval Board must approve any changes to the following service(s).
  ○ Remote Desktop Service

Collection of Information

Information that is collected from every device

• Operating system specifications, including version & patch status.
• List of applications, including name, version, patch status, aggregate usage statistics. Individual session information is not stored.
• Hardware specifications, including installed RAM, hard drive capacity, processor speed and type, BIOS information, serial number, warranty information, IP address, MAC address, etc.

Information that is NOT collected

The Endpoint Services applications are not capable of gathering or viewing certain types of information. Some examples of what cannot be gathered or viewed:

• Personally identifiable information
• Passwords
• Data files stored anywhere on the computer, particularly in users home folders,
• A list of files stored on the computer.
• Activities performed within an application, for example:
  ○ Browser history
  ○ Browser downloads
  ○ Keystroke logging
  ○ Opening, saving or closing of files
  ○ File change history
  ○ Any actions performed within the operating system, such as searching, saving, opening/closing of windows or files, settings changes, etc.
• HMS Endpoint Services applications CANNOT browse or “troll” data stored in any directory on the computer.

When Information is Collected
Inventory updates occur randomly within a 24 period.

**What HMS IT Will Do with Collected Information**

The HMS Information Technology Department may use this information to:

- Ensure the information stored on your computer is secure.
- Identify risks that could jeopardize information stored on your computer.
- Reduce time spent on resolving issues.
- Maintain a more complete inventory for security and business reasons.
- Enable HMS IT to be more proactive towards request and incident resolution.
- Enable HMS IT to identify existing support gaps, such as licensing new software or providing new services.

**What We Will NOT do with Collected Information**

The HMS Information Technology Department will not provide any gathered information to any group outside of HMS IT, except in an aggregate, de-identified format.

**Who will see this information?**

- Access to device specific information is limited to HMS IT Support Staff who have a demonstrated “need to know”, including the IT Service Desk and Client Services Representatives.
- “Need to know”: Support Staff are prohibited from providing any information to anyone other than other HMS IT Support Staff, and then only for the purposes of incident resolution.
- Requests for information submitted by Harvard University Office of General Counsel, Office of Research Compliance or Human Resources must be in writing and approved by the Director of Client Services or higher management authority.
- Aggregate data: From time to time, Harvard University Security and Compliance personnel may request reporting information on security compliance. This information is provided in a de-identified aggregate format.

Please view the [HMS IT Privacy Statement](#) for more information about who can access to your data.
Service Specific Terms

Inventory and Asset Management

The Inventory and Asset Management service provide a comprehensive hardware inventory as well as a limited software inventory.

- Inventory information gathered:
  Current hardware configuration, including Brand, model, CPU, RAM, Storage, serial number, MAC address, IP address, warranty status, BIOS information, and currently logged in user ID.
- Information collection cycle:
  Information is sent to the server approximately once every 24 hours in a secure encrypted format. Information is only sent while the computer is online. *Data that is sent contains only information about the hardware and software configuration.*

Software Self Service Portal

- The Software Self Service Portal provides a web or application based portal that can be used to install software. Applications within the portal are available to install at any time by the end user.
- Certain applications may require a license to be installed prior to installation or use of the application. The cost of the license will be noted in the description.

Application Deployment Service

- The Application Deployment service allows Support Staff to remotely install applications to your computer upon request.
- Support Staff will NEVER deploy software to your computer without your prior authorization.
- Applications that require a license purchase will not be installed until the license has been purchased.

Applications Available via Self Service and Application Deployment Service

- At a minimum, the following will be available at no cost to HMS Faculty, Staff and Postdocs:
  - Microsoft Office
  - Acrobat Reader
  - Backup software
  - Antivirus
- Other applications and resources may be made available at a future date.
- Certain applications may not be available to all users, depending on the user’s current status. Some applications may only be available to Faculty and Staff, while others may be available to On-Quad users.
- In order for applications to be installed, computers MUST be connected to the HMS Campus network either by Ethernet or HMS Private wireless or, if located off campus, via VPN Secure Network Connection.

Patch Management Service

- What updates will be pushed?
HMS IT Endpoint Services Program Terms of Service

- HMS IT may push certain Critical or Important OS, application or security updates to your computer automatically.
- We will make every attempt to notify the community at large of a pending software push. Occasionally, due to severe security vulnerabilities, we may be required to push a software update with little or no notice.

- When will updates be pushed?
  - Updates will be pushed after adequate testing, performed either in-house or by external sources.

- What devices will receive updates?
  - All devices enrolled in the Service and receiving software updates will be updated.

Encryption

It is the policy of Harvard University that ALL mobile devices that connect to or transmit data to or from Harvard University systems or over a Harvard University network must be encrypted.

** At this time, mobile device encryption is not enforced by HMS

More information is available on Information Technology's encryption web page:

- HMS owned and managed desktop computers are exempt from the encryption policy.
- Computers owned and/or managed by a hospital affiliate may have stricter enforcement policies. Those policies will be honored and enforced by the requesting affiliate. For example, some users who have appointment with affiliates with higher security standards may have a higher priority over HMS services, thus requiring devices to be encrypted. These devices must be handled on a case-by-case basis.

Questions? Call the IT Service Desk at 617-432-2000 or visit the HMS IT Web Site.
Remote Desktop Service

- Remote Desktop Service allows HMS Client Services Group Support Staff to initiate a remote desktop session to provide support services.
  - Access to the Remote Desktop Service
    - Only members of the Client Services Group have access to this functionality.
    - Access is restricted by department. CSR’s are only allowed to access computers within their respective support areas.
    - This Remote Desktop Service is for Service Desk Staff and Client Services Representatives only. For User remote access from an off campus computer to an on campus computer, please contact the HMS IT Service Desk or your CSR for assistance.
  - All Support Staff are required to close the remote desktop software at the end of each session.
  - Client Services Group IT Managers must request Remote Desktop privileges for each technician.
  - When Remote Desktop support sessions are initiated;
    - Client Services Group Support Staff will only initiate a Remote Desktop on a user device during support incidents initiated by the end user.
    - Certain devices, such as instrument computers, shared computers, kiosks or computer lab computers may not require end user initiation or authorization.
- Remote session authorization
  - Support Staff are unable to initiate a remote session without an end user present at the remote computer to authorize the remote session.
  - The end user must be present at the computer to authorize the remote session request.
- Remote session logging
  - All Remote sessions are logged. Logging includes who initiated the session, the remote (target) computer, the local host computer and when the session is approved by the remote user.
  - The service cannot log the activities performed during the remote session.
- Remote session security
  - All Remote Desktop session traffic is over secure HTTP or Secure SSH.
- Review and Changes to Remote Desktop Terms of Service
  - The Remote Desktop Service policy is subject to biannual review. Changes to this policy must be approved by the Service Owner, and the Director of Client Services.

Endpoint Management Service Objective

Through the use of industry standard software and tool, Endpoint Management services are intended to improve support levels and enhance the security and reliability of the computing environment within HMS.