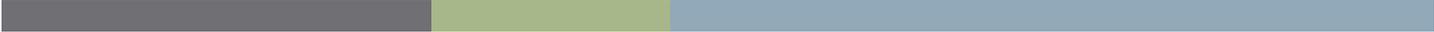


Technology Services,  
Loyola University Maryland



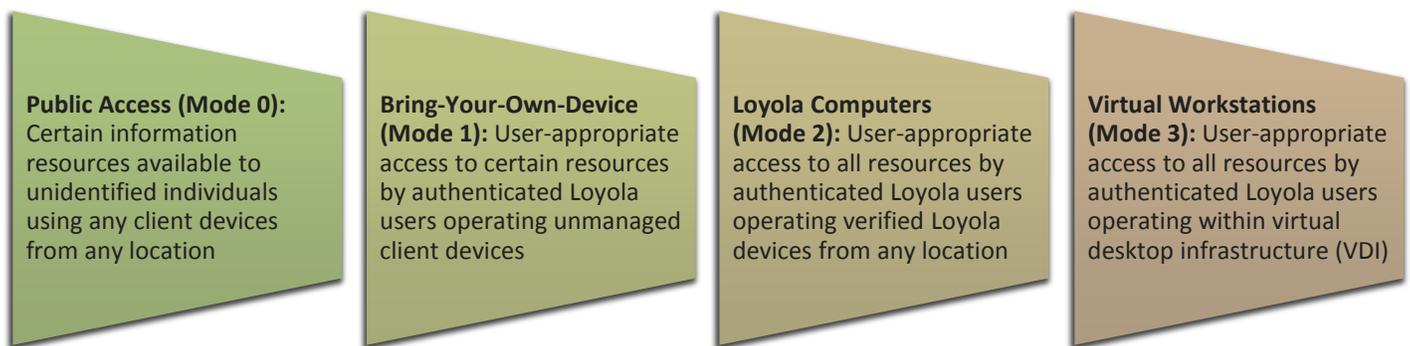
# Next Generation Client Computing Environment

The Future of Access

Draft September 9, 2013

## Modes of Access

In order to provide a consistent, seamless and secure end-user computing environment, Technology Services has identified four modes of access, which together provide our campus community with a comprehensive set of computing and access options.



Each of these modes is available to individuals according to their needs and preferences, but is of course dependent on the capabilities of their chosen client system (whether it's a Windows or OS X computer, or a mobile device like a phone or tablet computer) and on Loyola's security requirements.

### Seamless, Secure Access Regardless of Physical Location

Just like many other organizations, our community is increasingly mobile. Our faculty, staff, and administrators work from home or while on the road at conferences or training, and our undergraduate and graduate students need access to information systems from both on and off campus, while in the United States and around the world. We are dedicated to providing a consistent, full-featured computing environment that supports mobility and also protects Loyola from unnecessary risk.

### Modes of Access, Not Categories of Users

It's important to understand that each individual member of the campus community may use different modes of access at different times, depending on their needs.

An academic department chair, for example, may use a Loyola-issued laptop (Mode 2) when completing performance reviews of the faculty in her department, but may use a personally owned computer (Mode 1) from home to check her mail via Outlook Web Access. She may also check out events occurring on campus by accessing Loyola's public web site from a friend's computer (Mode 0).

An administrative department supervisor may use a Loyola virtual workstation (Mode 3) to access our Colleague system, but may later log into the Loyola portal from his personal iPad (Mode 1) to check on the progress of a project. The next day, he may use a dedicated, high-security Loyola computer (Mode 2) to access his patients' health information or to complete large financial transactions on the behalf of the University.

## Detailed Explanations of the Modes

**Public Access (Mode 0):** Some systems are accessible by anyone in the world, without needing to log in with a Loyola username. These resources are accessible from any Internet-connected computer or mobile device.

Example systems and services available: *www.loyola.edu*

**Bring-Your-Own-Device (Mode 1):** Students, faculty, staff, administrators, and certain other members of the Loyola community who have Loyola usernames are able to log in from unmanaged and personally-owned client devices to additional information resources not available to the public. Because Loyola has no control over the configuration or security of these computers and mobile devices, we need to balance our desire to provide access with our need to safeguard the data entrusted to the University by our students, employees, and others.

In addition to personally-owned devices, existing Loyola-owned computers and mobile devices that have not yet been configured, or are not able to be configured, to the appropriate level of our *Client Systems Security Configuration Standard* will be treated as unmanaged Mode 1 devices until and unless their configuration is verified and the device is authorized and authenticated.

Example systems and services available: *Loyola Portal, Outlook Web Access, Loyola's non-sensitive file storage service*

**Authorized Loyola Client Devices (Mode 2):** Depending on an individual's role at the University, he or she may be issued a Loyola laptop or workstation computer or a Loyola mobile device. After being configured according to the user-appropriate security level (high, medium, or low) of our *Client Systems Security Configuration Standard*, Loyola-owned client devices will be issued a client certificate. This certificate will enable the device to be authenticated for additional access beyond that available via to unmanaged devices.

This access will include a virtual private network (VPN) that provides authenticated users, operating authenticated devices, with user-appropriate access to all information systems from any location. Granular user access and privileges for individual information systems will not be managed by the VPN, but will continue to be provided via the role-based access controls of the individual information systems, as if the user were on campus. VPN access will be integrated as closely as possible with client operating systems, so that using it will be as easy and seamless as possible.

Example systems and services available: *Colleague Web UI, Informer, R25, Departmental file-shares, DSX, Outlook client, Titanium, Centricity, CSI payment card system, Loyola banking systems*

**Loyola Virtual Workstations (Mode 3):** Individuals and departments who prefer to use their personally-owned or publically available devices, but who need access to resources not available directly from unmanaged devices (Mode 1), may choose to use a Loyola virtual workstation. Referred to as Virtual Desktop Infrastructure (VDI), a Loyola virtual workstation is a Windows computer housed in our data center on shared hardware. It is accessible from any location on or off campus through an interface similar to Windows Remote Desktop or LogMeIn.

Properly authenticated users will be able to use a virtual workstation as if it were an on-campus physical workstation, but will be able to do so from any location and any capable client device. They will also have full user-appropriate access through VDI to all Loyola information resources. Since the virtual workstations are housed in Loyola's data centers, all user data in the VDI environment will be backed up daily. The security configuration and access control requirements for high, medium, and low security virtual workstations are covered in the *Client Systems Security Configuration Standard*.