Information Technology Services
University System of Georgia

Service Level Agreement
GeorgiaVIEW Learning Management System

University System of Georgia • Information Technology Services

Effective Date: 01/01/2015

Document Owner: Board of Regents of the University System of Georgia

Version	Date	Description	Author
2	01/30/15	Service Level Agreement	GeorgiaVIEW-Barry Robinson

By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.

Approvers	Role	Signed	Approval Date

CONTENTS

1. Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between the University System of Georgia – Information Technology Services also known as *USG-ITS* and GeorgiaVIEW (**V**irtual **I**nstruction **E**nterprise **W**ide) customers for the provisioning of IT services required to support and sustain the Learning Management System.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all IT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

2. Goals & Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent LMS service**,** support and delivery to the Customer(s) by the Service Provider(s).

The **goal** of this Agreement is to obtain mutual agreement for IT service provision between the Service Provider(s) and Customer(s).

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

3. Stakeholders

Information Technology Services (ITS) ensures an acceptable level of service by defining roles "IT Service & Support Provider," "Customer" and "User."

The following Service Provider(s) and Customer(s) will be used as the basis of the Agreement and represent the **primary stakeholders*** associated with this SLA:

- **IT Service and Support Provider(s): USG-ITS** ("Provider")
- **Customer**: Person or persons at University System of Georgia (USG) institutions or other USG related organizations who are authorized to conclude an agreement with ITS about the provisioning of the GeorgiaVIEW Learning Management System (LMS) and who are authorized on behalf of their institution or organization to contact ITS for GeorgiaVIEW LMS support. For the purposes of this document these individuals are referred to as GeorgiaVIEW LMS Administrators (primary, secondary, tertiary, etc) and are known to ITS and maintained with the USGTrackit customer profile and address book database. Others at USG institutions or USG related organizations may also contact ITS for GeorgiaVIEW LMS support, for example Chief Information Officer (CIO).
- **University of Georgia, Enterprise Information Technology Services**
- **User**: Person or persons who use the GeorgiaVIEW LMS system to conduct and execute routine learning or higher education activities (students, faculty, staff). It is

possible and acceptable that a USG institution GeorgiaVIEW LMS administrator (Customer) or ITS Helpdesk agent may play the role of "user" and contact the D2L End User Support Center.

*Additional **stakeholders** associated with this SLA include, but are not limited to, the taxpayers of the State of Georgia.

The following Service Provider(s) and Customer(s) will be used as the basis of the Agreement and Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **Business Relationship Manager** ("Document Owner") is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: USG-ITS
(Barry K Robinson)

Review Period: Yearly

Previous Review Date: N/A

Next Review Date: December 2015

4. GeorgiaVIEW Community

The following list includes main communications:

- Best Practices for Support and Communication
- Weekly Community Meetings
- GeorgiaVIEW Strategic Advisory Board– provides strategic advice to GeorgiaVIEW program
- GeorgiaVIEW Functional Advisory Committee – provides operational advice to GeorgiaVIEW program
- Stay in the Communications Loop with Information Technology Services Product and Service Status Updates program including subscription by institution within the Emergency Communication Service.
- ITS/GeorgiaVIEW will provide accurate, timely information to USG stakeholders via multiple communications channels as warranted & appropriate. The primary LMS administrator for each campus is updated weekly regarding current communication strategies and channels.

- Periodic LMS Administrator retreat opportunities. (Virtual and/or on-site)
- GeorgiaVIEW Admin Community within the LMS provides documentation and procedures. https://community.view.usg.edu

5. Learning Management System Environment

GeorgiaVIEW Brightspace by D2L License
The University System of Georgia has purchased a system wide license for the use of the Brightspace (excluding The Georgia Institute of Technology, Georgia Regents University and Georgia Southern University). GeorgiaVIEW received a considerable discount from the vendor.

GeorgiaVIEW Brightspace Production Environment (QPROD, XPROD)
Appropriate activities for the Production environment are:

- Course Creation
- Teaching
- Training
- Collaboration

The Production environments should not be used for:

Administrative tasks such as:

- testing new third party integrations
- testing external authentication
- testing SIS uploads

Expected Production environment upgrade periods: March (service pack upgrade), July (service pack upgrade), December (major version upgrade).

GeorgiaVIEW Brightspace Test Environment (QTEST, XTEST)
Appropriate activities for the Test environments are:

Administrative tasks such as:

- testing and training of new Service Pack and Version Upgrades

The Test environments should not be used for:

- Teaching**
- Course creation**
- Development**

**The Test environment will be overwritten with a copy of the Production environment just prior to the periodic upgrades. When this happens all data unique to the Test environment will be lost. Expected upgrade periods: March (service pack upgrade), July (service pack upgrade), September (service pack upgrade), December (major version upgrade). The TEST environment is expected to be cloned from Production prior to each upgrade and made available to the institutions for testing.

The Test (QTest and XTest) environments undergo maintenance nightly from 11:00 pm until 7:00 am the next day.

GeorgiaVIEW Brightspace Functional Development Environment (FDEV, KDEV)
Appropriate activities for the environments are:

Administrative tasks such as:

- Third Party Application Testing
- SIS Configuration and Testing
- External Authentication Testing
- Development (Course Widget, 3rd Party Applications, Web Services, Add-ons)

The FDEV environments should not be used for:

- Teaching**
- Course creation**

**FDEV and KDEV will alternate between having the current production version of the software and the future version of the software.

FDEV and KDEV undergo maintenance nightly from 11:00pm until 7:00am the next day.

GeorgiaVIEW Dependent Infrastructure Hardware and Services

Additionally, ITS will provide dependent infrastructure hardware and services necessary to host the Production and Test environments. These components include (virtual and physical): Network, Firewalls, Load Balancing, Application Servers, Database Servers, and Storage.

Process for Modifications to Hardware Infrastructure

When modifications to GeorgiaVIEW dependent infrastructure are deemed necessary, they modifications will be categorized as either 1. EMERGENCY or 2. STANDARD:

EMERGENCY Modifications: changes to infrastructure that are required immediately to prevent imminent issues on a broad scale many/all organizations. As much advance notification as possible will be provided to the customer via the Emergency Communication Service (ECS) to which all Admins are subscribe. All changes are reviewed by appropriate technical personnel. Post action details will be posted to:

http://status.usg.edu

STANDARD Modifications: changes to hardware, settings, and/or configurations that are required but can be scheduled. Notification of these changes deemed non-routine will be provided to the institutions via the weekly administrator's webconference and subsequent "Week in Review" document to the DAT-L listserv. These changes should be scheduled during a regularly scheduled maintenance for that instance. The desired amount of notification to the customer will be at least one week advance notice to provide opportunity for questions/concerns to be raised.

Disaster Recovery

Georgia*VIEW* Brightspace Application
System Component Failure Contingencies

Introduction

The purpose of this module is to describe procedures and standards for recovery plans to be implemented in the event of system component failures. The procedures described provide a structured recovery plan that is well documented and ready for execution when such extraordinary events occur.

Note: This module is not intended to document disaster recovery plans for catastrophic situations at Production Data Centers either at UGA or DB300.

Additional Note: This module pertains to the GeorgiaVIEW Brightspace Environment.

In such a recovery plan, two elements are necessary:

1. The parties responsible for particular components must know what management and users expect of them.

2. Interdependent groups must know what their expectations of each other should appropriately be.

For a failure contingency plan to be effective, it needs to be well documented and tested so that less time is spent figuring out the best way to invoke the contingency. From time to time, it also needs to be tested with each institution during normal operations so that we can have confidence that the contingency works and all parties involved have worked out any kinks in the process.

Topic 1: Servers

Servers

Each production instance of Brightspace is comprised of dozens of load balanced web servers and a Microsoft SQL Server cluster. The physical servers are under a 24 hours a day, 7 days a week, maintenance agreement with four hour response time. In order to limit the impact that any hardware failure will have on production services, the servers are configured as follows:

1. Each web server runs on a virtual machine hosted by a highly redundant VMware cluster. The database tier runs on a Windows and SQL Server clustered platform. The design is such that the failure of any physical server within the VMware cluster will have no impact on production. The loss of a physical server within the SQL Server cluster will cause only a slight pause in production while the secondary server automatically takes over. A utility node failure would require a manual intervention by ITS and Vendor.

2. Aside from internally mirrored system disks, all storage is provided by highly redundant, enterprise-class EMC storage arrays.

3. Each server is connected to the storage system by redundant paths provided by redundant switches and redundant storage controllers. The failure of any single path will have no impact on production.

4. A database failover cluster composed of both an active and passive host server of same specification backs each Brightspace application instance. Automated failover is initiated upon server/OS critical events and is seamless to the connectivity but with a minor delay in activity.

5. The active and passive database cluster nodes have redundant connections to all EMC disk paths which provide access to all of a clustered instance’s database filesystems from either host concurrently within a given production data center site.

6. Similarity in database server host platforms exists among all Data Center sites. This allows for replacement components to be sourced from development or other idle systems during critical production component failures.

   There are two options if system component failure requires active database operations to be relocated. The initial option is to utilize the configured failover policy to represent SQL Server components, filesystems and identity to the passive cluster host. This host is reserved for failover purposes and has full production resource capacity. In major disaster recovery scenarios where the cluster site itself is unavailable the last option would be to re-attach a database backup to the existing remote cluster instance assigned to the passive host of the target cluster instance pair. In the event of the complete loss of one site, ITS and Vendor would be required to rebuild service manually.

7. The production Microsoft SQL Server cluster instances are running in the Full Recovery model. This means that as long as regular backups are taken of the transaction log, a restore to a specific point in time can occur. The backups will be stored in the same location as the full backups on the data domain and will adhere to the same retention policy as the full and differential backups taken of the databases on each server.

8. Application access to the databases is handled through DNS, so that database access can be moved from one server to another without any required changes to application configuration.

Server Backups

The Backup and Retention schedule for database servers are as follows:

Database server backups are completed by the SQL Server Agent and written to and verified in the Data Domain. Full backups are taken once a day, differential backups are taken every 6 hours and transaction log backups are taken every 15 minutes except for between the hours of 6am and 8am. During this window is when the full backups are being taken.

- Database backups are maintained in the backup inventory up to seven (7) days from their creation.

Database server backups are completed via clustered SQL Agent jobs against the active SQL Server instance target. These backups are written to a redundant CIFS backup store. Transaction Logs are backed up in a similar process that writes to a redundant, networked backup store but at a higher daily frequency. Each of these backup routines runs daily and via the clustered OS scheduler.

The Backup and/or Retention schedule for web-application servers are as follows:

- Application nodes are backed up nightly.
- Application node backups are maintained up to five (5) days.
- Application Logs are maintained on the application node up to thirty (30) days.
- Network Activity Logs are maintained on a central logging server for up to fourteen (14) days.

Application server backups are completed via host backups of required filesystems through networked backup clients. These clients spool the backupset from the target application node to a central backup server responsible for scheduling and storage.

Backups from either Production Data Center are sent to their respective remote site, so that these backup sets will be in a location separate from the source data in case of an emergency.

Server Disaster Recovery

The Brightspace service's web tier and database tier are both redundant, and loss of any single server will have no real impact on production. In the case of the complete loss of one of the redundant database servers, system administrators would re-install the operating system on the replacement server and install the Microsoft software components necessary to add it back to the Windows cluster. Database administrators would then configure SQL Server and add the server back to the SQL Server cluster.

Backup Process (RPO):

Server backups are performed as outlined in the SERVER BACKUP section of the SLA. Backups from production services housed as UGA Boyd Data Center are stored remotely at the Daniel's Bridge Road location (DB300) in Athens, Ga. Backups from production services housed at DB300 are stored remotely at the UGA Boyd Data Center.

Recovery process:

In the event of a hardware stack failure, the maximum recovery time objective will be 24 hours. The maximum recovery point objective will be 24 hours.

In the event of a complete and indefinite failure of one of our two primary sites in Athens, GA due to power, internet connection or other environmental factors, the maximum recovery time objective will be dependent on the following factors:

1. Emergency order of hardware to complete the primary site stack.
2. Installation of hardware at remote site
3. Installation on application on database and application node tiers by vendor (D2L)
4. Linkage to backup data

Every effort will be made to work with each party as quickly as possible in good faith to minimize the RTO timeframe and meet reasonable best practices. If an institution wishes, ITS will ascertain the additional costs associated with building out a remote "warm" site and identify a specific RTO.

EMC Enterprise Storage Systems

Both the databases and associated content rely on EMC enterprise-class storage arrays. Through maintenance agreements, EMC provides proactive monitoring of this infrastructure 24 hours a day, 365 days a year, and dispatches service technicians to correct problems as necessary.

EMC Enterprise Storage systems provide the highest degree of data protection and continuous availability. These systems are fully protected against planned or unplanned disruption of information availability and accessibility. The architecture features mirroring, hardware redundancy, and non-disruptive microcode upgrades and component replacement. These systems also feature a full-system battery, which guarantees no lost writes and orderly transitions or shutdowns during power outages. Extensive proactive and predictive intelligent maintenance features, such as cache and disk scrubbing and an integrated Remote Maintenance Processor (RMP), add to the information protection and continuous information availability features.

Database Servers

This document does not address information on database component failure because those scenarios are addressed as database recovery actions rather than disaster recovery. Database backups are kept for disaster recovery purposes, and are to be used to recover the entire database in the event of a failure. These backups are not intended to be used to recover specific data for an institution. However standard database backup and recovery practices that include a combination of frequent database backups and full recovery models utilizing Transaction logs are being used as part of a comprehensive database recoverability strategy.

Risk Assessment

Based on past history, failure events such as these may be most likely to occur due to:

1. Physical database server failure
2. Prolonged power outage at either the UGA or DB300 computing center.

Recovery Scenarios

1. **Physical database server failure**

The database tier is clustered such that loss of a physical server will have no real impact on production. In the case of the loss of a *primary* database server, there will be a slight pause in production while the secondary server automatically takes over.

2. Prolonged power outage at either computing center.
Scenario:

UGA or DB300 sites lose power for an extended period of time, exceeding one hour.

Response:

The Georgia*VIEW* systems are supported by UPS systems at each production site. The UPS can most likely support the servers long enough for the system administrator(s) to perform the emergency shutdown procedures gracefully in the event of a long-term power outage. There are also facilities to re-route main electrical supply from up to three regional utilities if the issue is one of supply.

Responsibilities

For any server problem, whether it is something small or something catastrophic, please request support by contacting the **ITS HELPDESK**.

Topic 2: System Software and Databases

In the event of massive data corruption, System Administrators are prepared to replace any and, if required, all of the following system and database software components. Brief procedural descriptions are provided.

Operating System

System administrators would use Windows Deployment Services and associated PowerShell scripts and group policies to install pre-configured versions of Windows Server on both the web and database tiers, as required.

Databases

The Logical Volumes specific to a database server would be created by the System group based on what was originally set up for the database server.

After the storage has been presented, the Brightspace DBA group would decide based on last known good backup what files to use to restore back to the closest time possible to the corruption event.

Responsibilities

For any database, application server, or process scheduler technical problem, whether it is something small or something catastrophic, please request support by contacting the **ITS HELPDESK**.

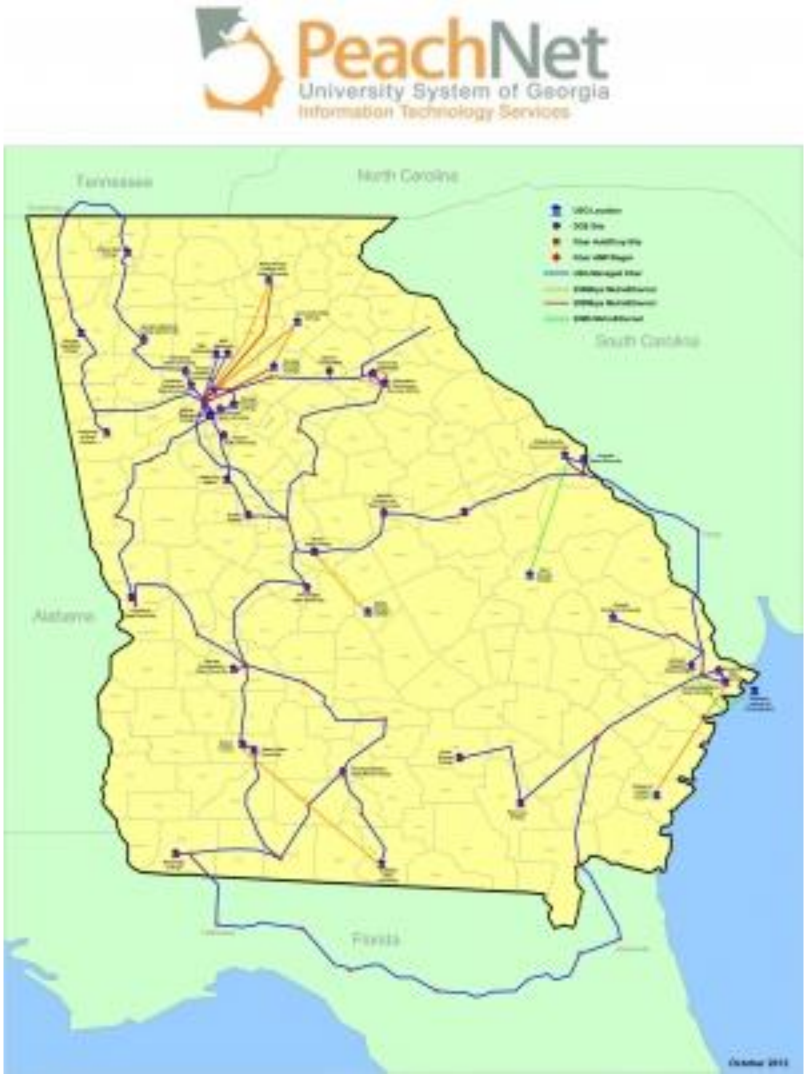
Topic 3: Networks

Local Area Networks (LANs)

It is the responsibility of each institution to operate and maintain its own Local Area Network(s).

Wide Area Network

PeachNet is the Wide Area Network (WAN) used for Georgia*VIEW*. It is the responsibility of ITS Network Support Services to operate and maintain PeachNet. The figure following shows the current PeachNet backbone.



Emergency Measures

In the recent past, ITS/EIS/NSS and WSS (Workstation Support Services), along with ITS/EAS/TS (Enterprise Applications Systems/Technical Services), have worked together to devise innovative solutions, enabling ITS/EIS/NSS to respond to emergencies that have occurred due to WAN failures based on the approach of providing alternative connectivity such as PPP dial-in, Out-of-Band Contingency systems or local execution of needed tasks..

While these measures have been successful, this approach is the least functional contingency plan, because it can only be used if an institution is in certain steps of its processing. We have been very fortunate to date that we have not experienced a case where data entry was incomplete at the time of a WAN failure. It must also be noted that in these cases quite a bit of time was spent deciding how to work around the network failure and configuring a workstation on both sides to deal with the FTP transfer.

Risk Assessment

Based on past history, failure events such as these may be most likely to occur due to:

1. Lack of sufficient available bandwidth to run any processes within an acceptable length of time.
2. WAN circuit failure to site.
3. Failures in the core 0 area causing lost connectivity to PeachNet.
4. Configuration errors in the core 0 area causing lost connectivity to PeachNet.

Recovery Scenarios

In emergencies such as these, the institutions that have found themselves in crisis have been at a point in the payroll process that allowed us to execute emergency measures such as these successfully:

1. **Lack of sufficient available bandwidth to run any processes within an acceptable length of time.**
   Scenario: An institution lacked sufficient available bandwidth to run any processes within an acceptable length of time.

   Response: ITS ran the required processes from Athens and FTP'd the output back to the institution's file server for printing and electronic distribution. There was sufficient bandwidth for FTP.

2. **WAN circuit failure to site.**
   Scenario: Failures in the WAN circuit caused an institution to lose connectivity to PeachNet.

   Response: Again, ITS ran the processes on the server side. This site hosts a local PPP dial-in service, so that service was used to connect to their LAN via dial-up and FTP'd the output back to a server on-site.

3. **Failures in the core 0 area causing lost connectivity to PeachNet.**
   Scenario: Failures in the core 0 area caused an institution to lose connectivity to PeachNet.

Response: Again, ITS ran the processes on the server side. This site hosts a local PPP dial-in service, so that service was used to connect to their LAN via dial-up and FTP'd the output back to a server on-site.

4. **Configuration errors in the core 0 area causing lost connectivity to PeachNet.** **Scenario:** Configuration errors in the core 0 area caused an institution to lose connectivity to PeachNet.

   Response: ITS ran the necessary processes on the server side and used HyperTerminal to connect to a local desktop and deliver the necessary output.

Responsibilities

For any network technical problem, whether it is something small or something catastrophic, please request support by contacting the **ITS HELPDESK.**Topic 4: Application Support

Introduction

The purpose of this module is to outline the approach to customer service and support provided by the Information Technology Services (ITS) to University System of Georgia (USG) institutions using the Georgia*VIEW* hosted applications.

Service Level Guidelines (SLG) for ITS Customer Support

ITS provides central support to USG institutions and GALILEO/GIL customers for ITS products and services. The efficient operation and service of these products requires that ITS and its customers share and understand support procedures, roles and responsibilities, lines of communication, and expectations. In order to insure an acceptable level of customer support, ITS established consistent and efficient processes and procedures that are outlined and defined with the **Service Level Guidelines (SLG) for ITS Customer Support** document.

The Service Level Guidelines document defines the processes and procedures that guide support goals and objectives. It is based on the two-way conditions of customer requirements and support center capability. From a high level it defines, but is not limited to, the services offered, severity and priority levels, response and resolution (target) times, and the methods customers will use to request services.

More specifically, the SLG outlines USG institution customer support. It is an outline of support methodologies, processes, and guidelines and is not a contractual agreement in any form. As such, best practices outlined in the SLG reflect ITS's processes that:

- Have formed over time to provide customer support; and,
- Are based upon support industry best practices and methodologies.

The **Service Level Guidelines (SLG) for ITS Customer Support** document is located at the URL below: http://www.usg.edu/customer_services/guidelines/.

Requesting Support: Contacting the ITS HELPDESK

To submit:

- A new non-emergency, non-production down support request, please use the self-service support request options available through the ITS Customer Services web site at: http://www.usg.edu/customer_services.
- An update to an existing support request ticket/case, please e-mail helpdesk@usg.edu and include the ticket/case number
- A production down, emergency support request, please call 1-888-875-3697 (toll free within Georgia) or 706-583-2001.

For further information on **ITS HELPDESK** support communication guidelines, customer self-service, hours of operation and contact information, procedures for off-hours support, and procedures to engage ITS support resources for an emergency, please refer to the **Service Level Guidelines (SLG) for ITS Customer Support** document noted above.

6. LEARNING MANAGEMENT SYSTEM INTEGRATIONS

Student Information System Batch Integration
The Brightspace batch integration process provides campuses with the ability to load Brightspace compliant xml files into the LMS through a bulk load process.

Campuses will submit files via the GeorgiaVIEW Moveit File Transfer Utility (MFT) at

https://files.usg.edu

Student Information System file downloads received through the GeorgiaVIEW MFT before 8:00pm on an ITS business day are loaded into GeorgiaVIEW Brightspace by 9:00am the next business day. SIS data files received by 8:00pm Friday are loaded into GeorgiaVIEW Brightspace by 9:00am the following Monday. ITS reserves the right to load Friday's file before 9:00am Monday morning.

Schedule adjustments and exceptions to accommodate inclement weather days, Board of Regents' holidays, and announced Board of Regents' furlough days might be required. Announcements will be posted through program specific mailing lists (DAT–L).

Data files submitted through INGRESS will be processed on a nightly basis with the exception of scheduled maintenance periods.

Questions regarding missing or incorrect course, section, user, or enrollment data related to the integration process should be directed to the GeorgiaVIEW Integration team.

Brightspace External Authentication (if selected)
GeorgiaVIEW will work with campuses to troubleshoot issues related to local external authentication efforts by testing campus provided test accounts and test systems and assisting in the review of any necessary settings through the user interface. USG will support external authentication methods that are supported by Brightspace.

All communication with LDAP servers must be done over an encrypted channel using LDAPS on port 636. We require that SSL certificates be issued by a 3rd party certificate authority. Due to security risks we do not allow the use of locally generated SSL certificates but require all SSL certificates to be issued by a 3rd party certificate authority.

3rd Party Integrations (existing through implementation)
GeorgiaVIEW will work with campuses to troubleshoot integration related issues involving the settings, functionality related to integration with the LMS, and provide vendor related documentation (where appropriate) to assist campuses with 3rd party vendors as it relates to the integration. Campuses should contact the vendor for issues related to software functionality. Primary LMS Adminstrators for each institution can view validated integrations in the GeorgiaVIEW Admin Community at the following URL: https://community.view.usg.edu under Integrations.

ITS and GeorgiaVIEW do not have control of all content and communications where Brightspace is integrated with a third party vendor. It is important for campuses to fully understand the risk of using a vendor where the content is hosted outside of the Brightspace ILP, and campuses assume that risk when integrating a third party product.

7. Learning Management System Performance & Escalations

Availability	**Client Escalation Procedures**
≥ 99.9%	N/A
≥ 99.5% to 99.9%	Escalation to GeorgiaVIEW Director and Institutional Primary Administrator

≥ 99% to 99.5	Escalation to Institution CIO and System CIO
≥ 98% to 99%	Escalation to USG Chief Academic Officers and Institutional VPAA
< 98%	Escalation to USG Chancellor and Instiutional President

Availability, in number of outages/year	**Client credit (annual)**
<=2 Priority 1 Issues *	N/A
3-4 Priority 1 Issues *	Escalation to GeorgiaVIEW Director and Institutional Primary Administrator
5-6 Priority 1 Issues *	Escalation to Institution CIO and System CIO
7-8 Priority 1 Issues *	Escalation to USG Chief Academic Officers and Institutional VPAA
9-10 Priority 1 Issues *	Escalation to USG Chancellor and Instiutional President

- Excluding announced maintenance event (emergency or planned), when announced at least 4 hours before to the event.

For details, refer to the

· USG Service Level Guidelines (http://www.usg.edu/customer_services/service_level_guidelines)

· ITS Maintenance Schedule (http://www.usg.edu/information_technology_services/learning_in_21st_century_georgia/georgiaview/maintenance_schedule/)

8. SECURITY

1. The Board of Regents is responsible for protecting the information of the institution that is stored in the hosted Brightspace system including the implementation of reasonable and prudent access controls, settings and threat management technology.
2. The hosted Brightspace product will have all security-related patches applied within two weeks of release.
3. ITS Individuals with administrative access will be in positions of trust within the Board of Regents that have been subject to checks and vetted according to Board of Regents practices.

4. Any administrative access to the Brightspace platform that grants access to institutional data protected by FERPA will be approved by the institution. ITS and D2Lhave pre-approved access in the event of an institutional support request or urgent instance issue.
5. Administrative access to the Brightspace system will be reviewed regularly by Board of Regents management.
6. Applying the principle of least privilege, no individual will have administrative access to the hosted Brightspace system without a requirement for that access to perform their job duties.
7. Vulnerability assessments will be performed by or facilitated by the Board of Regents at least annually. The institution will be notified of any vulnerability as the Board of Regents becomes aware of them in a timely fashion.
8. The Board of Regents will maintain reasonable and prudent security monitoring of the Brightspace system to detect intrusion and/or data exfiltration. The institution will be notified of any exposures of information as the Board of Regents becomes aware of them in a timely fashion.

9. LEARNING MANAGEMENT SYSTEM SUPPORT

GeorgiaVIEW provides USG institutions with an integrated learning platform: Brightspace by D2L. It supports both on-campus and off-campus learning experiences through a framework offering communication, resource access, testing, and management that serves the learning and communication needs of faculty, students, and administration.

GeorgiaVIEW is the comprehensive program to manage the services associated with the centrally hosted Brightspace. This program includes the management of the USG Brightspace license; support of each campus utilizing the centrally hosted system, setup and maintenance of the centrally hosted centers, integration efforts, project management, planning, training, and service upgrades.

GeorgiaVIEW develops resources to support campus adoption and use of D2L, including training and support materials for students, faculty, and administrators. GeorgiaVIEW seeks to achieve a higher standard of minimum hosting and application capabilities as well as achieve the economies of scale associated with developing a critical user mass and leveraging expertise across the University System.

The statewide Brightspace license covers all uses of Brightspace for faculty, staff, and students including any uses for Continuing Education. Campuses are encouraged to utilize Brightspace, not only for academic purposes, but also for faculty training, staff development, student services, etc. The potential uses are only limited by the creativity of the campuses.

The URL for each USG institution (*.view.usg.edu) must remain accessible for support personnel.

Technical Support (GeorgiaVIEW/ITS)

The ITS Service Level Guidelines (SLG) ensures that an acceptable level of support service is defined for and provided to USG institutions and customers through ITS, as set forth and governed within and by the

ITS/USG Service Level Guidelines (SLG)
http://www.usg.edu/customer_services/service_level_guidelines/

More specifically, the SLG outlines customer response, resolution, and support channels of communication that the vendor/partner agrees to follow. It is an outline of support understanding, methodologies, processes, and guidelines and is not a contractual agreement in any form. As such, best and good practices and standards outlined herein reflect ITS processes that

- Developed over time, with input from ITS, USG institutions, customers, and in collaboration with vendor/partners to provide customer support

- Are based on support industry best and good practices, standards, and methodologies

The processes described within the SLG are subject to change as ITS matures and improves customer support.

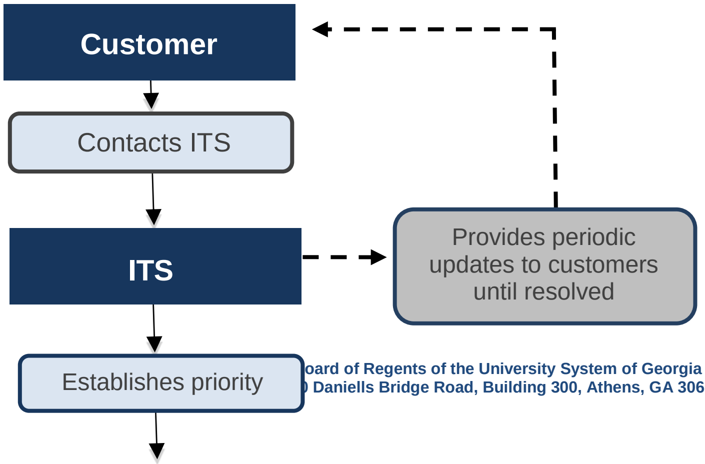
Service Request
A service request is a proposal from a Customer or User for new or enhanced GeorgiaVIEW LMS product, support, or service. For example, there may be times when a Customer or User requests new capabilities, enhanced or changed functionality for any of the GeorgiaVIEW LMS service area.

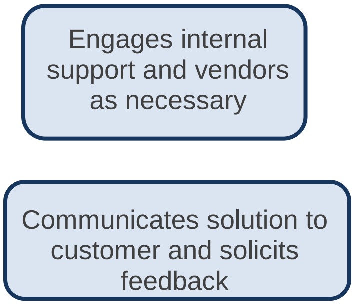
GeorgiaVIEW LMS service requests can be submitted at this website:

ITS Customer Services
http://www.usg.edu/customer_services
(see Submit Service Request Here button)

Note
Production downs or business interruptions that impact changes should be reported by Customers according to standard procedures detailed within the Customer Support section and ITS SLG.

ITS Customer Support/Service Request Process



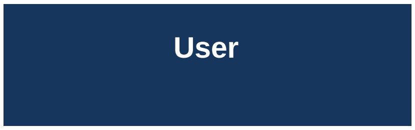

Engages internal support and vendors as necessary
Communicates solution to customer and solicits feedback

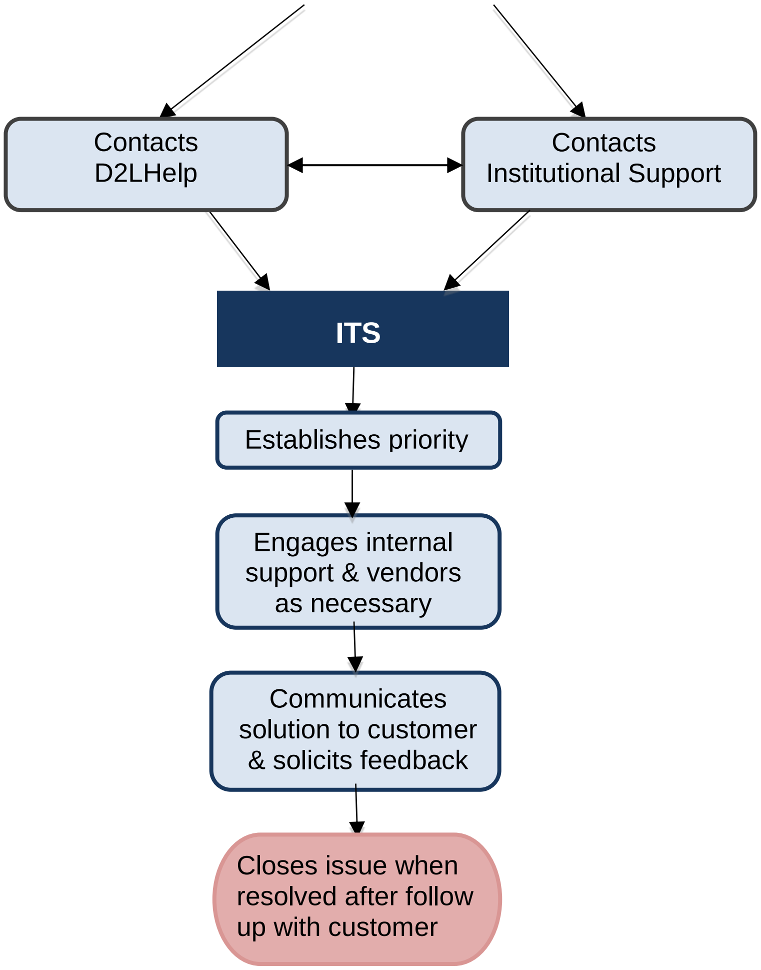
Functional Support (End-User)

An acceptable level of functional, end-user support is provided to all GeorgiaVIEW Faculty, Students, and Staff through the Brightspace Premium Plus End User portal referred to as GeorgiaVIEW D2L Help Center (DHC). The DHC website (https://D2LHelp.view.usg.edu) provides a searchable, self-service knowledge base of support topics, as well as dedicated, toll-free phone numbers for real-time assistance- 24 hours a day, seven (7) days a week, 365 days a year.

Support is available to record issues, explain the functions and features of the Brightspace software, and clarify the contents of any D2L documentation. The DHC strives to resolve all generic (non-bug) problem tickets in a single phone call or email within 15 minutes and typically provides, at a minimum, an 80% resolution on first contact. For those problem tickets that cannot be resolved within that time frame, the problem is escalated and the appropriate amount of resources will be allocated to assist in the resolution of the problem. These service level responses are intended to be a general guideline of expectations for providing service to end users. If the DHC is unable to resolve a request in a reasonable length of time, or if the priority or severity of the request changes due to external factors, the request will be escalated to GeorgiaVIEW, or as necessary. D2L support may request additional information to assist in the understanding of the problem. Escalation may require further research by the Help Desk, consultation of other D2Lsupport staff members, and/or consultation with the D2L development team. Customers should not use Support for services other than Support. Services including training, implementation, modifications, configuration, and communications, will be charged at the Rates given in the Master Agreement, except for out-of-pocket and per diem expenses.

User Support Process




Contacts D2LHelp
Contacts Institutional Support
ITS
Establishes priority
Engages internal support & vendors as necessary
Communicates solution to customer & solicits feedback
Closes issue when resolved after follow up with customer

Brightspace Premium Plus Support
See D2L Master Agreement, Support Schedule

10. LEARNING MANAGEMENT SYSTEM SERVICE AVAILABILITY

Stay in the communication loop with Information Technology Services (ITS) GeorgiaVIEW Brightspace service status changes, updates, maintenance schedules, and other service interruptions.

Service Status

Information Technology Services (ITS) makes it easy to know the status of, and receive updates about University System of Georgia (USG) Information Technology Services products and services including GeorgiaVIEW Brightspace

Information Technology Services (ITS) Services Status announcements:

http://status.usg.edu

USG Service delivery uptime data is available here:

https://www.usg.edu/uptime/

ITS provides customers with the best level of service by using a variety of communication methods to share information about the operational status of supported products and services, and makes it easy to choose the communications option that works best for you.

For more information about communication options for product and service status updates, visit

ITS Customer Service web site: http://www.usg.edu/customer_services/

and select the Stay in the Communications Loop with ITS Product and Service Status Updates

Quick Link (http://www.usg.edu/customer_services/documents/Stay_in_the_Communications_Loop_6.pdf).

Maintenance Schedules

ITS designates maintenance schedules for GeorgiaVIEW Brightspace hosted services every other weekend, during which the GeorgiaVIEW service may be temporarily unavailable. These schedules define periods that are used to perform upgrades, apply patches or security releases, perform system backups, and other routine tasks that help to avoid unscheduled or unexpected service interruptions or outages.

For detail information about GeorgiaVIEW Brightspace maintenance schedules refer to the

- Master ITS Maintenance Schedule (http://www.usg.edu/information_technology_services/learning_in_21st_century_georgia/georgiaview/maintenance_schedule/)

- GeorgiaVIEW service entry including times and the More Information link below

Notes:

- Depending on the activities to be carried out, it may not be necessary for ITS to use all of the scheduled time posted for GeorgiaVIEW Brightspace environments described within the ITS Maintenance Schedule

- ITS reserves the full maintenance period at each maintenance occasion

- Should a maintenance schedule extend beyond an end time posted within the ITS Maintenance Schedule for GeorgiaVIEW Brightspace, or extend beyond a pre-arranged and mutually agreeable end time for additional maintenance, ITS will communicate these changes through the communication options described in the Stay in the Communications Loop with ITS Product and Service Status Updates procedure and tools

Additional Maintenance

On rare occasions, ITS may schedule in advance and perform maintenance activities outside of the schedules described above.

When these events occur ITS will publish these changes in advance through the communication options described in the Stay in the Communications Loop with ITS Product and Service Status Updates procedure and tools.

These communications will include special announcements with specific details regarding the services, sites, and/or clusters affected and associated time frames.

Unscheduled and Emergency Maintenance

When the stability of a service is deemed to be at risk, ITS may declare an unscheduled or emergency maintenance event.

Unscheduled and/or emergency maintenance events can occur outside of or during normal ITS business hours including evenings, weekends, Board of Regents holidays, or an ITS closure including inclement weather conditions.

- Customers will be notified of these events and status updates are provided in advance whenever possible and practical.

- If an unscheduled or emergency maintenance is of such short duration that it is not possible or practical to provide advance notification, ITS will always provide a Post Action notification and summary through the Stay in the Communications Loop with ITS Product and Service Status Updates procedure and tools.

More Information

For details, refer to the

- USG Service Level Guidelines (http://www.usg.edu/customer_services/service_level_guidelines)

- ITS Maintenance Schedule (http://www.usg.edu/information_technology_services/learning_in_21st_century_georgia/georgiaview/maintenance_schedule/)