



Service Level Agreement (SLA)

Between

*[Add your department and acronym (I)] Technology Systems Division (TSD)
Information Technology Unit (ITU)*

and

XYZ

For XYZ Service

TSD and XYZ Service Level Agreement

Document Version History

Version #	Date	Revised By	Reason for Change

TSD and XYZ Service Level Agreement

Table of Contents

1	General Overview	1
2	Service Description.....	1
2.1	Service Scope	1
2.1.1	<i>User Requirements.....</i>	2
2.1.2	<i>Boundaries of Service Features and Functions</i>	2
2.2	Service Level Performance	2
2.2.1	<i>General Service Levels.....</i>	2
2.2.2	<i>Specific Service Levels</i>	2
3	Roles and Responsibilities	2
3.1	Service Providers and Customer Contacts	2
3.1.1	<i>Service Providers.....</i>	2
3.1.2	<i>Customer Contacts.....</i>	2
3.1.3	<i>Customer Data Owner.....</i>	3
3.2	Service Provider - Data Center Co-location Responsibilities.....	3
3.3	TSD-ITU Responsibilities.....	3
3.3.1	<i>Network Connectivity.....</i>	3
3.3.2	<i>Network Security.....</i>	4
3.3.3	<i>Backup and Recovery</i>	4
3.4	Customer Responsibilities	5
3.3.1	<i>System Management and Security.....</i>	6
4	Methods of Requesting Service	6
5	Hours of Coverage, Response Times and Escalation	6
5.1	Hours of Coverage.....	6
5.1.1	<i>Implementation Scheduling.....</i>	6
5.1.2	<i>Service Availability.....</i>	7
5.1.3	<i>Incident Support Hours, Response Times, and Reporting.....</i>	7
5.1.4	<i>Prioritization</i>	7
5.1.5	<i>Service Requests.....</i>	7
5.2	Escalation	7
5.2.1	<i>Scheduled Service</i>	7
5.2.2	<i>Service Level.....</i>	7
5.3	Information.....	8
5.4	Other Requests	8
5.5	Service Exceptions to Coverage.....	8
6	Maintenance and Service Changes	8
7	Pricing	10
7.1	Pricing Process	10
7.2	Charges	10
8	Reviewing and Reporting	10
8.1	System Performance and Availability Reporting.....	10
9	Description of Co-located Equipment	11
10	Security Agreement and SLA Approvals.....	11

1 General Overview

This is a Service Level Agreement (SLA) between (*insert customer org name*) and the Technology Systems Division of the Information Technology Unit Data Center to document:

- The technology services Data Center Co-location provides to the customer
- The targets for response times, service availability, and maintenance associated with these services
- The responsibilities of Data Center Co-location as a provider for subscription based services, hourly services or specific services
- Processes for requesting services
- Review and Reporting SLA process
 - This SLA will be reviewed annually to assess hardware, software and procedural accuracy.
 - This SLA shall remain valid until revised or terminated

2 Service Description

2.1 Service Scope

- TSD-ITU provides co-location services in the campus Aquia Building Data Center. The service provides customers with a secure location and network connectivity for housing mission-critical servers and related equipment. The campus Data Center is a hardened facility that provides a precision environment for the housing of mission-critical servers and related equipment. The facility is connected to the campus backbone network via (example: two separate 10-Gigabit trunks) for high availability. Customers are provided rack space in lockable cabinets with dual power connections, backup UPS, remote management access for servers, hardware installation assistance, and staffed Data Center Operations Desk.

The collocation service also includes:

- Equipment rack space in lockable cabinets.
- Electrical connectivity with dual power connections; centralized UPS and generator will provide continuous power in the event that commercial power fails.
- Hardware installation assistance.
- Use of data center network infrastructure (redundant gigabit Ethernet to campus backbone).
- Intrusion detection systems deployed at the campus network border to the internet.
- Remote management access.
- Physical security and access control.

TSD and XYZ Service Level Agreement

- Automated 24x7 monitoring for environmental conditions and security.
- Use of facility loading dock, freight elevator, and carts.

2.1.1 User Requirements

- *(Each co-location customer will have unique requirements to list here)*

2.1.2 Boundaries of Service Features and Functions

- *(List boundaries/Limits to service – unique to each customer)*

2.2 Service Level Performance

- See Service Metrics template measured levels *(Insert link to Metrics template.)*
- See GMU Systems Status and Metrics page:
[http://itservices.gmu.edu/services/metrics/.](http://itservices.gmu.edu/services/metrics/)

2.2.1 General Service Levels

- *(List non-measured levels.)*

2.2.2 Specific Service Levels

(See Service Providers) (Insert link to Service Providers section.)

- *(List measured levels.)*

3 Roles and Responsibilities

3.1 Service Providers and Customer Contacts

(List Service Providers who will support this agreement and represent the primary TSD stakeholders associated with this SLA)

3.1.1 Service Providers

The following Service Provider(s) are associated with this SLA *(add/delete rows as necessary to identify providers)*:

Service Providers	Title / Role	Contact Information*
Technology Systems Support (TSS) <i>(enter specific name/s)</i>	<i>Enter Title/Role here</i>	<i>[Enter Contact Information]</i>
Technology Systems Support (TSS) <i>(enter specific name/s)</i>	<i>Enter Title/Role here</i>	<i>[Enter Contact Information]</i>

3.1.2 Customer Contacts

The following *Organization Name* personnel are associated with this SLA *(add/delete rows as necessary to identify customer contacts)*:

Customer Contacts	Title / Role	Contact Information*
<i>Customer Org Name (enter customer specific name/s)</i>	<i>Enter Title/Role here</i>	<i>[Enter Contact Information]</i>

TSD and XYZ Service Level Agreement

<i>Org (enter specific name/s)</i>	<i>Enter Title/Role here</i>	<i>[Enter Contact Information]</i>
<i>Org (enter specific name/s)</i>	<i>Enter Title/Role here</i>	<i>[Enter Contact Information]</i>

3.1.3 Customer Data Owner

Data may be Sensitive, Protected or Public Data as defined by Policy 1114, Data Stewardship. The Data Owner is responsible for all data in their purview (see section 10) (*there should be only one Data Owner*).

Customer Data Owner	Title / Role	Contact Information*
<i>(enter data owner's name)</i>	<i>Enter Title/Role here</i>	<i>[Enter Contact Information]</i>

3.2 Service Provider - Data Center Co-location Responsibilities

Data Center Co-location responsibilities and/or requirements in support of this Agreement include:

- Meet response times associated with the priority assigned to incidents and service requests.
- Review Service Level Agreement annually and notify customer of updates or changes.
- Appropriate notification to Customer for all scheduled maintenance via the TSD-ITU System Alerts and Outages page: <http://itservices.gmu.edu/alerts/>.
- Data Center Co-location group will implement defined processes to deliver these service levels.

3.3 TSD-ITU Responsibilities

TSD-ITU will provide the infrastructure, technology, people, processes and monitoring tools necessary for Data Center Co-location and:

- TSD-ITU provisions server racks in lockable cabinets.
- TSD-ITU provides redundant power, UPS, and generator backup.
- TSD-ITU provides 24x7 automated monitoring of environmental and physical security.
- TSD-ITU will work with customer to help rack, cable, and label equipment.
- TSD-ITU provides secure building access; entry is card-key controlled, and restricted to pre-authorized users who have undergone police background checks.
- TSD-ITU will, in limited situations, reboot servers based on customer request.
- TSD-ITU provides staffed service desk (see Hours of Coverage).
- In the event of power or unanticipated network issues, TSD-ITU will notify Customers within **x** hours of event occurrence.

3.3.1 Network Connectivity

(Edit the following as needed for each customer)

- TSD-ITU provides network connections for equipment and IP addresses as required. TSD-ITU is responsible for ensuring network connection to campus backbone (and Internet).
- Network demarcation: TSD-ITU manages and will troubleshoot all network equipment from the campus border.

TSD and XYZ Service Level Agreement

- Router up to the patch panel connection in the Data Center rack to which the customer's equipment is attached.
- This includes the TSD-ITU-supplied cable connected to the patch panel and used to plug into the customer's equipment. The Customer is responsible for managing and troubleshooting all user installed servers and equipment (i.e., end devices).
- TSD-ITU provides remote management access via **Keyboard Video Mouse (KVM)** or serial console for servers located in the Data Center.

3.3.2 Network Security

(**Edit** this section as per needs of each customer)

- All customers collocating equipment in the Data Center are required to place the equipment behind the Data Center provisioned firewall. Customers requiring more than 3 IP addresses will be placed on a **separate subnet**, with their own virtual firewall instance.
- TSD-ITU will maintain hardware, OS upgrades and patches for the firewall. All network connections will be placed on the virtual Local Area Network (**vLAN**) for the customer's subnet, accessible via the firewall.
- Customers placed on their own **subnet** are responsible for administering the configuration of the virtual firewall and its rule sets. Customers requiring fewer than 4 IP addresses will be placed on a shared collocation subnet. TSD-ITU manages the configuration rule sets for firewalls on the shared subnets.
- TSD-ITU provides intrusion detection at the campus border. Internal traffic is not monitored. However, TSD-ITU Security scans the campus network for potential threats and will alert departmental security contacts for corrective action.
- TSD-ITU reserves the right to block any server that it believes poses a serious threat to campus computing resources or the Internet. This may involve a compromised host or one identified as causing severe performance issues affecting other nets. Guidelines for determining this course of action and notification procedures can be found at (add link)
- TSD-ITU manages a **Restricted Data repository** of all systems using restricted data governed by SB 1386, FERPA, or HIPAA. Customers must register with the RDM. The TSD-ITU Security team can provide security and tools to help secure machines using restricted data.

3.3.3 Backup and Recovery

(**Specifics** should be edited for each customer and are for example only)

- TSD-ITU can provide secure backup through the GMU Backup service (describe service here). The client can optionally enable a feature to encrypt the data stream between the client and backup server.
- The customer is responsible for maintaining the encryption key password; if you lose the password, your encrypted data cannot be recovered. Be sure to keep a copy of the password in a location different from the server being backed up.

TSD and XYZ Service Level Agreement

- The service performs daily incremental backups (after initial full backup). Backups are **retained for up to five of** the most recently modified versions of files, so that older versions can be restored. Deleted files can be recovered up to **30 days** after deletion
- TSD-ITU maintains off-site storage containing updated copies of all backed-up files for added protection.

3.4 Customer Responsibilities

Customer responsibilities and/or requirements in support of this Agreement include (these are examples – add/delete as needed for each customer):

- Customer will abide by the [Aquia Data Center Physical Security Policy](#) (this is a new policy on M:\shared\TSD-ITU.clientrel\Gail's Policy Folder)
- Customer representative(s) must be available when resolving a service related incident or request.
- Communicate specific service availability requirements.
- Submit service requests through appropriate trouble ticketing system, contact telephone numbers for new services or technical support.
- Maintain current hardware warranties and software license agreements.
- Prompt payment.
- Designated department-billing contact.
- Customer will only use rack space allocated to customer.
- Customer may not 'lease' this space to other customers.
- Customer agrees to coordinate with TSD-ITU placement of new or relocation of existing equipment.
- Customer agrees to orient equipment in a manner that complies with the hot aisle/cold aisle airflow plan for the given location. TSD-ITU will work with the Customer to ensure compliance.
- Customer is responsible for paying for all costs and expenses associated with all devices and peripherals, software, maintenance and associated vendor relations.
- Customer pays for network drop, rack space, firewall context, and (if requested) backup service.
- Customer must ensure that equipment meets established industry electrical, thermo, and magnetic standards. TSD-ITU will request removal of any equipment out of compliance with established standards.
- Customer ensures delivery of equipment to the Data Center.
- Customer provides rack-mount kits for equipment.
- Customer provides asset tracking of customer-owned equipment.
- Customer uses TSD-ITU-supplied cables.
- Customer provides and ensures that system and security contact information is kept up-to-date.
- Customer subscribes to <http://itservices.gmu.edu/alerts/> for GMU network related announcements (e.g., security alerts, planned and unplanned outages, maintenance calendar, etc.).

TSD and XYZ Service Level Agreement

-Customer complies with Data Center policy for controlled access; only pre-authorized users are granted access. Cardkey access is not to be shared or transferred.

3.3.1 System Management and Security

(These are examples – add/delete for each customer)

-Customer is responsible for all hardware and software maintenance, systems administration, and monitoring of collocated equipment.

-Customer is responsible for managing the configuration and rule sets of the hardware firewall service module if their equipment is placed on a dedicated subnet in the Data Center.

-Customer is responsible for staying in compliance with Responsible Use of Computing University Policy 1301 (<http://universitypolicy.gmu.edu/1301gen.html>).

-Customer is responsible for registering servers using restricted data in the Restricted Data Management repository ([link](#)).

-Customer is responsible for investigating any reports of potential security vulnerabilities involving customer's equipment, and, if necessary, removing the offending device from the network.

Security violations will escalate as appropriate. If necessary, TSD-ITU may need to shut down connection to the server until customer is able to verify that the system has been re-secured.

4 Methods of Requesting Service

- Online via Service Desk Express (SDE)
- Submit a Data Center Co-location Request Form F0055
- Phone via ITU Support Center (703-993-8870)
- Email (itusupport@gmu.edu)
- Walk-in (ITU Support Center)
- Negotiation with Service Provider

5 Hours of Coverage, Response Times and Escalation

5.1 Hours of Coverage

-The Data Center normal hours of operation are (example follows) 6:00 a.m. to 12:00 a.m., Monday – Friday except Federal holidays, University holidays, and announced University closures. Data Center Co-location provisioning requests will be completed or scheduled within one (1) business day after receipt of notification during normal business hours. Customers may use any of the methods of contact outlined in Section 4.

-After hours, requests submitted will be processed during the next business day.

5.1.1 Implementation Scheduling

New Data Center Co-location services and capacity upgrades are scheduled during normal business hours:

-x a.m. to x p.m., Monday through Friday, except University or government holidays

TSD and XYZ Service Level Agreement

5.1.2 Service Availability

Service availability defines the percentage of time this service is available, with the exception of scheduled maintenance, and within service availability hours.

-x a.m. to x a.m., Monday through Friday, excluding holidays

5.1.3 Incident Support Hours, Response Times, and Reporting

(These are examples to be edited for each co-location customer)

A Data Center Co-location incident is any interruption or malfunction of normal functions. The Data Center Co-location's incident support hours are **24** hours per day, **365** days per year. The Data Center Co-location's technical contacts will respond to an incident within ninety minutes (90) after receipt of notification from the Service Desk via any of the methods outlined below:

To report a Data Center Incident, please email or phone the TSD-ITU Service Desk at:

-Email: support@gmu.edu

-Telephone: 703-993-8870

TSD-ITU Service Desk is staffed from x a.m. – x a.m. Monday through Friday, and x a.m. – x p.m. on weekends. (These hours may be subject to future changes. Changes will not result in reduced customer access to collocated equipment).

5.1.4 Prioritization

The Data Center Co-location group will prioritize incoming incident requests as “urgent” priority if it meets any one of the following criteria:

- Number of departments or people affected.
- Percentage of total tasks that can no longer be performed by individuals.
- Academic and Administrative Calendar deadlines.
- Impact on the delivery of instruction.
- Lasting impact on student academic performance.
- Risk to safety, law, rule, or policy compliance.

5.1.5 Service Requests

A service request means a request made by a customer to the Data Center Co-location Group for a service. Service requests will be processed after receipt within one (1) business day, Monday – Friday, x a.m. to x p.m., excluding holidays.

Service Request changes will be made during service request support hours.

To request Co-location Services (e.g., to request a managed firewall service instance) please create a ticket using the following method: email at support@gmu.edu or call the Support Center at 703-993-8870

5.2 Escalation

5.2.1 Scheduled Service

If a service request is not implemented or scheduled with the response times outlined above, customers may escalate the request by contacting the TSD-ITU Service Desk at 703-993-8870. Please refer to the service request ticket number before contacting.

5.2.2 Service Level

If you are not satisfied with the level of service on a request, contact the TSD-ITU Service Desk at 703-993-8870 or email support@gmu.edu. Escalation requests are categorized and processed as appropriate.

TSD and XYZ Service Level Agreement

5.3 Information

Assistance for all IT Services is available through the [ITU Support Center](#):

Phone: 703-993-8870

Fax: 703-993-3347

E-mail: support@gmu.edu

Online: [Submit a Request](#)

Hours of Operation: Monday thru Friday, 8 a.m. – 7 p.m.

Walk-in Support Innovation Hall, Room 233
Fairfax Campus*: Monday thru Friday, 8:30 a.m. – 5 p.m.
(*closed Thursdays 3 p.m. – 4 p.m. for team meetings)

Howard Davis
Manager, Aquia Data Center
hdavis12@gmu.edu
703-993-3385

5.4 Other Requests

Requests for service features and functions not yet implemented can also be submitted via TSD-ITU Service Desk at 703-993-8870 or email at support@gmu.edu

5.5 Service Exceptions to Coverage

Federal Holidays: (to be identified)

University Holidays: (to be identified)

Scheduled Maintenance(s): Scheduled between Data Center Co-location, Technical and Data Owner Contact: No coverage

6 Maintenance and Service Changes

The Change Management process within Data Center Co-location minimizes unintended service disruptions or other impacts to the Campus as a result of changes in the production environment. Data Center Co-location does this by monitoring, managing, and evaluating changes to maximize the service benefits to the customer, while minimizing the risks involved in making those changes. Please note that some maintenance work may cause service disruptions.

TSD and XYZ Service Level Agreement

All Data Center Co-location related services, maintenances, and Campus outages are published at TSD-ITU Alerts and Outages page, <http://itservices.gmu.edu/alerts/>. Additional detailed information can also be found on the GMU Systems Status and Metrics page: <http://itservices.gmu.edu/services/metrics/>.

There are three categories of service changes:

- 1. Planned Maintenance:** Planned service maintenance is approved work that is planned and scheduled prior to the change. Data Center Co-location will communicate (as needed) to the appropriate department contacts prior to the scheduled change. Whenever possible, schedule maintenance is planned during off-hours on weekends, and performed as necessary in the quickest and most efficient manner to ensure restoration of affected services. Planning for outages includes careful reference to the academic calendar to ensure the mission of the University is not affected. No planned network maintenance will occur during scheduled finals weeks, the first week of each semester, or at other critical periods. Regularly schedule maintenance is performed 6:00 a.m. – 12:00 p.m. every (indicate day). Email and website notification at <http://itservices.gmu.edu/alerts/> will be sent with the date and time of the planned maintenance window, scope of impact, and potential effects of the outage to campus parties potentially affected by the event.
 - a. GMU ISP, Campus Backbone Media or Core Routers**
 - Outage duration: less than 15 minutes**
 - Required completion: before 7:00 AM, 7 days per week
 - Minimum notification: 48 Hours (not counting weekend hours)
 - Outage duration: greater than 15 minutes**
 - Required completion: before 7:00 AM, 7 days per week
 - Minimum notification: 72 Hours (not counting weekend hours)
 - b. GMU subnet(s) - (if implemented)**
 - Outage elapsed time: less than 15 minutes**
 - Required completion: before 7:00 AM, weekdays or as negotiated with departments for weekends
 - Minimum notification: 24 Hours (not counting weekend hours)
 - Outage elapsed time: greater than 15 minutes**
 - Required completion: before 7:00 AM, weekdays or as negotiated with departments for weekends
 - Minimum notification: 36 Hours (not counting weekend hours)
- 2. Unplanned Maintenance:** Unplanned production maintenance is priority work that is unplanned due to an urgent repair, patch or update to prevent failure. Unplanned production maintenance will be given priority (and communicated immediately). Critical patch notification is determined by the nature of the problem and may be scheduled in less than one day. As such, critical security or

TSD and XYZ Service Level Agreement

break-fix patches are applied as needed. If possible, Data Center Co-location will email the Technical and Data Owner contacts as soon as possible to coordinate the application of these patches.

- 3. Emergency Service Change:** An emergency service change is defined as a service failure that affects the entire campus or significant number of users that requires immediate repair, and is performed as necessary and in the quickest and most efficient manner to ensure restoration of affected service. All Emergency Service Changes are communicated to the appropriate Data Center Co-location contacts to determine necessary communication steps. An email notification describing the problem, scope of impact, and resolution will be sent to <http://itservices.gmu.edu/alerts/>) and to other campus parties affected by the event as appropriate. Emergency service announcements are also communicated usually the day of the service failure. Off-hours service failures are communicated the following business day.

7 Pricing

7.1 Pricing Process

Software licenses and associated maintenance fees will be set at the current market rate negotiated between Data Center Co-location and the vendor. Any set-up fee rate changes will take effect on Month/Day x, at the beginning of the new fiscal year.

7.2 Charges

In succeeding years, customers will be billed in July, following the start of the new fiscal year, and billed monthly thereafter. Customers may terminate the service at any time without charge with 30 days advance notice. No refunds will be issued for unused Data Center Co-location. Any billing questions should be directed to ([Link](#)).

8 Reviewing and Reporting

8.1 System Performance and Availability Reporting

This Agreement is valid from (*date*). The 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 service provider(s) 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 service provider(s) will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Metrics monitored internally for this service are listed in Section 2.2. Reporting on these metrics will take place (*daily, monthly, quarterly*) and made accessible on the internal service web page.

TSD and XYZ Service Level Agreement

This Agreement will be posted to the following location and will be made accessible to all stakeholders: Document Location (add link)

9 Description of Co-located Equipment

Describe in this section – list will be unique for each customer (or add to Appendices)

10 Security Agreement and SLA Approvals

The Administrative Data Stewardship Policy Number 1114 applies to all academic and operational departments and offices at all George Mason University locations, owned and leased. This policy defines Highly Sensitive Protected Data and Restricted Protected Data, as well as Public Use data. The policy also defines the Data Owner as the person responsible for ensuring that University data security policies are followed and for developing internal controls to ensure data security and privacy.

The data associated with the TSD-XYZ SLA is governed by this policy and is defined as (select each data set type that applies):

☐ Highly Sensitive Protected Data

☐ Restricted Protected Data

☐ Public Use Data

Appendix C of Policy 1114 includes authorization procedures and forms that require the user to state the business need and agree to accept the responsibility to protect the highly sensitive/restricted data. Any university employee, student or non-university individual who stores highly sensitive university data without proper permissions and protection measures is in violation of this policy and will be subject to appropriate disciplinary action, including possible dismissal and/or legal action.

The Unit and Department Liaisons and ITU Senior Managers approve this document. The customer will be provided the signed copy for their records. Then, the signed document is stored in the TSD's Administrative Suite, Room 249, the Aquia Building, and published in the password-protected section for SLAs on TSD's web site.

The terms of this SLA are effective as of the period of performance: the date approved and signed by all parties below until *(add date 1 year from dated signature)*. Any changes to the data sets covered by this SLA that occur during the period of performance shall require an immediate revision to this SLA.

I agree with the terms of this Service Level Agreement. I have read and complied with Data Stewardship Policy 1114. I will continue to monitor any data set changes and will comply with my responsibilities as per University Policy 1114. Specifically, I will review potential data set changes with the IT Security Office and notify TSD of proposed

TSD and XYZ Service Level Agreement

changes so that this SLA may be revised prior to implementation of the data set modification.

Approval Signatures:

Director
(add your department), TSD, ITU

Date

Phone:

Email:

Director
Customer Organization

Date

Phone:

Email:

Review:

Executive Director
TSD

Date

Phone:

Email:

Appendix A – Monitoring Details

Equipment Monitoring Details of MEC's Systems

Quick View (*add a photo/image of the rack with location*)

Appendix B – XYZ and TSD Contacts

XYZ Authorized Contacts

The following individuals have been authorized by the XYZ management to contact the ITU to request support services provided through this SLA:

TSD and XYZ Service Level Agreement

TSD Contacts

John Kettlewell Director Technology Support Services Phone: (703) 993-3358 Email: jkettlew@gmu.edu	

Appendix C – Itemized Costs