Service Level Agreement

for

Computing Services

at the

UC Davis Graduate School of Management

Purpose

This Service Level Agreement (SLA) meant to establish a framework and cooperative partnership between the Graduate School of Management Information (GSM IT) and its customers by clarifying roles, setting expectations, and providing mechanisms for resolving problems. It will identify the roles and responsibilities of all participants and define the types and levels of computing support and service available at the Graduate School of Management (GSM).

This agreement is intended to guarantee that all faculty, staff, and students receive an acceptable level of service for their information technology needs. GSM IT is committed to providing a high level of service and ensuring information technology is an effective and enabling tool for its customers. GSM IT service goals are:

- Support the educational mission of UC Davis and the GSM
- Establish clear and reasonable service expectations
- Create and maintain a standard automation platform for accomplishing specific business tasks
- Provide a standardized and secure database structure for managing information.
- Maintain a secure and reliable computer network environment
- Provide timely and effective technical support to GSM staff, faculty, and students
- Implement cost efficient technology that effectively supports business and educational needs of the GSM
- Establish a process for software development of supportable applications in accordance with UCD Policy & Procedure
- Establish a staff development program that develops and maintains necessary technical expertise within the school

This document is intended to be a living document and will be continually updated to address organizational changes, availability of new technology, and fundamental technology strategies of the school.

Standards & Conventions

Standards and conventions reduce the total cost of technology within the University and leads to increased support efficiencies. Implementation of standards and central coordination of computing equipment acquisitions will produce economies of scale in purchasing, simplify the acquisition process, provide greater leverage in negotiating support terms, facilitate hardware and software deployment, and facilitate training of technical staff and users.

GSM IT is dedicated to providing efficient support for a standard suite of recommended business solutions, but cannot effectively support a proliferation of hardware/software. Customers are encouraged to choose from the standards and conventions outlined in this document (see Appendix B), which will be reviewed and updated on an annual basis.

Administrative Computing Plan

GSM IT will align services and promote solutions conforming to the Campus Administrative Computing Plan. The Plan describes the general framework governing administrative computing at UC Davis. It includes a description of principles, system standards, systems, analyses, and

processes that promote alignment and guide development of specific solutions to computing requirements.

Campus Network Infrastructure

The mission of the UC Davis Information and Educational Technology (IET) department is to create and support an information technology environment that enhances the ability of the UC Davis community to teach, do research, and provide public service. It strives to deliver an infrastructure of technological services appropriate to the requirements of the campus community.

The GSM IT Director (or designee) will participate in campus-wide technology committees.

The GSM IT will capitalize on the UC Davis network infrastructure and services to the greatest extent possible, including, but not limited to:
- Campus Computing Accounts
- Use of Network Access Modules that provide access the Campus network back-bone.
- Use of the campus secure wireless network solution.
- Use of centralized Domain Naming Service (DNS)
- Use of centralized Dynamic Host Configuration Protocol (DHCP) services
- Campus Active Directory and Exchange Services (uConnect)
- Campus Virtual Private Networking (VPN) for secure remote access

Use of the wired network will be limited to full-time faculty and staff and will require pre-registration of equipment network serial number (i.e., Media Access Control (MAC) address). The GSM IT group will enter device MAC address in the Campus InfoBlox system for full-time faculty and staff upon request, or as routine during system deployment. Systems added to the wired network must University owned equipment and be Cyber-Safety compliant (per UCD PPM 310-22). Mobile devices (cellular, laptop, tablet, etc.) will not be allowed to operate the GSM wired network; they will be limited to the campus wireless network.

Network access by visiting and adjunct faculty, visiting lecturers, students, and guests will be limited to wireless connectivity via the Campus wireless system. Use of this system requires a Campus computing account. Sponsors of visitors will arrange for guest computing accounts through the Campus (http://wireless.ucdavis.edu/guestaccess.cfm).

Help Desk

The IT Help Desk serves as a centralized point of contact for all computer issues to enable the GSM IT group to provide quality service. All requests for computer installations, maintenance, problem resolution, system changes, or related questions for any of the systems, or technologies listed in this document should be directed to the GSM IT Help Desk.

> GSM IT Help Desk
> 752-4660
> helpdesk@gsm.ucdavis.edu
> Monday-Friday 9AM to 5PM
> (excluding holidays)
> *Walk-in hours: M-F, 9am-10am & 1:30pm-2:30pm*

Due to liability and policy issues, the GSM IT group can only provide service on University property and can only service University owned equipment.

The GSM IT Help Desk will be staffed during the hours cited above. You are welcome to submit questions to the help desk outside these hours, by leaving a voicemail or sending e-mail. We will respond to your needs as soon as possible. Extended service is available by special arrangement, but is contingent upon GSM IT staff availability. Sufficient advanced notification, generally one to two weeks, is required for scheduling purposes.

Network Operations Schedule

The GSM IT group strives to ensure that all network hardware and software is operational 24 hours a day, 7 days a week. All equipment is normally available at all times except when essential maintenance to hardware or software is required. If it is necessary to interrupt any service, prior notification will be given and, whenever possible, interruptions are scheduled to minimize their impact. Additionally, if individuals encounter problems, they are encouraged to report the problems to the GSM IT Help Desk.

Issue Tracking & Service Priorities

A unique tracking ID will be assigned to all service requests and logged in a call tracking database system. The status of any call can be obtained by calling or emailing the GSM IT Help Desk.

The GSM IT group will prioritize all requests, which cannot be immediately resolved, to ensure an appropriate response based upon the priority guidelines below. The GSM IT staff will ensure that customers are apprised of the status, and in all cases, notify the customer when the request is resolved. The customer will receive an automated response when a ticket is submitted to the help desk. The customer will receive an update at least every two weeks if the ticket has not yet been assigned to a technician. Once assigned, the technician will provide status updates at least monthly.

The method within the GSM Issue Tracking system for identifying service request priority is named "Urgency" and will be used prioritize requests based upon their perceived criticality. ***Requests are addressed based upon the Urgency, then on a first in, first out basis***

- **Urgency 10 - Emergency:** Problems affecting multiple users and causing a work stoppage for a large group or entire staff. IT staff will begin working on the problem immediately. IT staff will notify senior staff of the status on a regular basis until the issue is resolved or a definite timeframe for resolution can be determined. Examples of a Urgency 10 service request includes: a server hardware failure, failure of department-wide software program/service (i.e., VPN, Application Server, RaPS, EMS, etc), email system outage, failure of computer labs while a training class is in session, or failure of classroom A/V equipment.

- **Urgency 8/9 – Work Stoppage:** Problems causing a work stoppage for a single user. IT staff will begin working on the problem within two hours (assuming staff is not already assigned to a higher priority). IT will provide a status on resolution regularly until the issue is resolved or an estimated timeframe for resolution is identified. Examples of urgency 8/9 problems include: complete failure of a computer or monitor, or employee relocation due to environmental emergency. This does NOT include new user requests (ref: the Routine section).

- **Urgency 5-7 – Disruption**: Problems interfering with the timely and effective work of an individual, or problems directly impeding the instructional mission of the school. IT will begin working on the problem as soon as possible. Examples of urgency 5-7 problems include: inability to use a particular software package, or software application problems; or classroom operational issues. Faculty support issues will generally be assigned as urgency 7, unless timely repair is not an issue (e.g., planned replacement of computing equipment where timing does not affect instructional mission).

- **Urgency 2-4 – Routine**: Scheduled services and/or projects. The timeframe for these requests will be handled when practical, based upon existing work backlog and staffing availability. Examples of urgency 2-4 issues include: new/updated access to network services or software, installation of a new computer, printer problems, computer equipment move, audio/visual setups, consulting services, software/system development.

- **Urgency 1 – Incoming**: New requests are automatically assigned this level, which will be generally reviewed by the IT staff within 1 business day and changed to the appropriate level.

- **New User/Employee Account/Equipment Requests** - New user account requests are initially considered Routine. Supervisors should anticipate the potential delay and submit the request well in advance of the employee's start date (i.e., best to address immediately after offer is accepted). Urgency l will be increased over time based upon the following criteria:
    - Routine: Initial request. A minimum of 1 week notice prior to employee's start date is expected.
    - Disruption: After employee's start date, but not sooner than 1 week after initial request
    - Work Stoppage: After employee's start date, but not sooner than 2 weeks after initial request

Equipment Physical Access

GSM IT uses remote access utilities to the greatest extent possible to assist its customers. If the user workstation is configured with firewall protection, then the firewall settings must be configured to allow access from the GSM IT Help Desk systems.

If on-site service is required, then IT prefers to work on computer equipment when the customer is present. This ensures that the customer has an opportunity to confirm the problem is corrected. Occasionally, IT staff must enter a work area when the customer is not there. IT will do this only when one of these conditions apply:

- The customer requests that IT staff perform the work in their absence.
- The customer, or their department's management, has given IT staff access to the office to complete a time-sensitive repair or installation.
- The IT staff is responding to a security issue.

System Administrative Access

Administrative access is necessary to support computer systems. The IT staff is prohibited by Campus policy from using standard user accounts to perform administrative functions. Likewise, users are prohibited by Campus policy from divulging their user account password for use by others. As such, any system to be supported by GSM IT needs an administrative level account dedicated for IT staff use. Windows systems should be configured to be a member of the GSM Active Directory domain*, so the IT staff can use the existing Domain Administrator account. Non-Windows systems should be configured with a local system account with full administrative privileges for IT staff.

Administrative level access is generally not provided to staff unless a specific need is identified (i.e., needed to operate a specific software application). Administrative level access is generally provided to faculty as most faculty purchase and install their own software applications. Anyone provided administrative level access must comply with UCOP BFB-IS-3, Electronic Information Security, and UCD PPM, Section 310-22, UC Davis Cyber-Safety Program. The UC Davis Cyber-Safety Program requires users to only use privileged accounts when performing administrative functions (i.e., installing software, or using a program that requires administrative access) and will otherwise, use a non-privileged account.

*Note: Registering a computer to be a member of the Active Directory domain offers distinct advantages including increased administrative capabilities by GSM IT and reduced vulnerability to malicious internet activity.

Service Catalog

A wide variety of computing services (see Appendix A) are offered to all faculty, staff, and students. These services will be reviewed and updated periodically.

Basic Network Services

GSM IT will establish and administer basic network services for the GSM as defined in Appendix C.

Computer System Standards & Support

Support will be provided for all standard hardware and software configurations and non-standard configurations where support for such configurations has been negotiated and defined through a specific service level agreement (SLA).

For full support, staff and faculty must use standard hardware and software configurations that GSM IT recommends. In some cases, faculty/staff may choose to use configurations not recommended or supported by this standard service level agreement. Support for these configurations must be negotiated with the GSM IT Director and the resulting agreement approved by both parties. GSM IT reserves the right to recommend that support for some configurations be provided by outside vendors.

Software Support

GSM IT installs and maintains a wide range of computer software for client and server platforms (as identified in Appendix C). Typically, only current versions of evaluated software are installed on computer equipment. GSM IT reserves the right to make changes to the list of supported or non-supported software at any time. GSM IT will conduct required troubleshooting of any problems or issues that arise, and assist with making effective use of these software tools.

GSM IT is generally focused on installing and maintaining software configurations, not software use. Software use and training is generally the responsibility of the user.

GSM IT makes every effort to cross-train its staff in the support of software systems. However, the reality is – given the rapid change in information technology and available resources – it will never be possible for each member of the IT staff to be fully knowledgeable about the intricacies of all the software used throughout the GSM. GSM IT staff are committed to doing as best possible. In situations where an emergency or departure of key department staff requires that GSM IT troubleshoot specialized applications, extra time may be necessary to address problems that arise.

Installing Software

GSM IT strongly recommends that computer users do *not* load software themselves on their computers. Many software packages make changes to system configuration files, which can conflict with existing configurations and result in other software not working properly. GSM IT reserves the right to discontinue support and/or un-install user-installed software (or hardware), especially when it interferes with other hardware/software installed on the user's workstation.

Software installation requests will generally be considered low priority. Problems that arise as a result of user/self-installed software (without consultation from GSM IT) will fall to the bottom of the priority list and will be addressed as time permits.

Software Development, Administration, and Support

GSM IT performs software development as designated and prioritized by the Assistant Dean of Administrative Services in coordination with the GSM IT Governance Committee. On-going development, administration, and support will be defined by separate Service Level Agreement (SLA) or Memorandum of Agreement (MOU).

Software Developed by External Service Providers

Due to various circumstances, it is sometimes necessary to contract out system/application development to a third party. **In such cases, it is *strongly* encouraged to utilize GSM IT as a consulting resource** – to, among other things, review and validate technical specifications, test plans, program listings and documentation, upgrade/modification procedures, service level agreements for ongoing support and maintenance etc.

Software development and system implementation generally requires system administrative access to GSM computers/data. Please review/coordinate your needs with the GSM IT group in advance of establishing any contract.

As a general rule, GSM IT does not support software developed by external service providers. However, support can be negotiated with GSM IT, provided that adequate training is provided to IT staff, and GSM IT is involved in reviewing and signing off on the deliverables mentioned above.

Sorry, but the GSM IT staff are prohibited from working on non-University owned equipment. So, there are only two choices available to get software installed on your personal computers:

- Do it yourself. This method is preferable, and many of the more commonly used software programs on the market today come complete with easy to use 'Install Wizards' to guide users through the set-up process.
- Commercial computer repair/support vendor

Purchasing New/Replacement Computer Systems

The following guidelines have been established for new/replacement systems:

All Computer Equipment

All computer related purchases (i.e., hardware/software) must be processed through GSM IT to ensure it meets minimum Cyber-Safety compliance when deployed and meets established standards identified in appendix B. This includes any computing device that will be connected to the UC Davis network (i.e., computers, printers, PDAs), any software, and any accessories over $500.

Faculty Computer Equipment

Funds for computing equipment, software, and services is included in the recruitment package. GSM IT will coordinate with the new faculty member to determine appropriate and reasonable system configuration (i.e., desktop, laptop, peripherals, etc.).

Faculty should be prepared to replace computers at least every 4-5 years with a system meeting latest minimum specifications. Replacements will be funded through RATS account or other funding negotiated with the Dean.

Staff Computer Equipment

GSM deploys AWS Workspaces for staff. AWS Workspaces is a virtual Windows desktop cloud-service that allows staff to work with a consistent experience from any location. Workspaces can be accessed from any computing device.

Staff will be provided one computing device and appropriate accessories (i.e., 2 monitors, keyboard, mouse, web-camera, and headset) for accessing their Workspace. If an employee is assigned a desk at the GSM, then a desktop computer with the accessories will be provided for that location. If the employee is allowed to work remotely and not assigned a desk, then a desktop computer or laptop (employee's option) with the accessories will be provided for their home office. Staff that are provided equipment for their home office can utilize any available "hoteling" (i.e., temporary shared) office space office if they are working on-prem. Employees that are provide a hybrid work schedule and are assigned a desk will be responsible for providing any additional needed equipment for their home office. All equipment provided the employee will be configured for accessing their AWS Workspace; additional software will not be installed, except for security/administrative utilities designated by the GSM IT unit.

GSM IT will replace computing equipment as needed with a system meeting latest minimum specifications. Replaced computers will be designated as surplus property and is not eligible for cascading (i.e., hand-me-down) to other employees. Cascading and maintaining older equipment significantly increases support costs and places an undue hardship on IT resources.

First time equipment for a staff position will be funded by the employing unit. The IT unit will cover the replacement cost on a designated cycle that meets the appropriate life-cycle for the type of equipment issued. The IT unit will also cover the cost of non-functioning equipment.

Staff that have a regular business need for travel can be provided a laptop that will be configured to access their AWS Workspace. While Internet service is required to access a Workspace, it is generally available in most locations. If Internet access is not expected, then the employee should be provided an "Internet Hot-Spot" device or "Tethering Service" on their University owned cellular phone. The cost of this extra equipment is to be approved by the employee's supervisor and funded by the employee's unit.

Internet Service Provider (ISP) services, associated network equipment, and printers for home offices is the responsibility of the employee and is not covered by the GSM, except as approved by the GSM Dean's office. The GSM IT unit cannot assist in the setup or support of home networks and equipment.

Student Computer Equipment

Student equipment is not provided by the GSM. The GSM requires students to have the following:
- Laptop computer less than three years old
  - A Dell Latitude series laptop is recommended to ensure complete compatibility with the GSM wireless network and print services.
  - Access to a Microsoft Windows operating system
  - Access to Microsoft Office "for Windows".

The Dell Latitude is only a "recommendation" to ensure that student equipment is 100% compatible with the GSM network infrastructure. If students purchase the recommended Dell, then GSM IT will go to every extent possible to ensure the laptop works properly with our equipment. With that said, students can opt to use a Mac, as many students do. However with a Mac, students must accept the following:

1. Students must meet the requirement to have access to a Microsoft Windows environment. You can achieve this by running VMWare, Parallels, or bootcamp on the Mac, then installing Windows <u>and</u> Office. Or, if the student has access to a different PC (i.e., at home/work), then it will minimally suffice. The reason for this requirement is that students will be required to run some statistical software packages that ONLY run on Windows and not Mac. Also, students will be required to use some statistical Excel plug-ins that do not work on the Mac version of MS-Excel.

2. If students encounter problems with the wireless network or GSM printers, the GSM IT staff can only offer minimal assistance to help resolve issues. The IT staff is quite knowledgeable with Apple products, but simply don't have the resources to keep up with the idiosyncrasies of all computer manufactures and

12

their various system drivers, so can't spend excessive time helping students resolve potential issues.

Computer Repair

If a computer requires repair, GSM IT will recommend appropriate course of action. Generally, GSM IT does not perform computer component repair. GSM IT reserves the right to replace systems in order to resolve a problem as quickly as possible.

Ownership of Obsolete, Excess, and Surplus Property

All obsolete, excess, and surplus property (e.g., phased-out hardware) becomes the property of GSM IT. GSM IT will disassemble retired hardware/software configurations and make use of any spare parts or other components that are in good operating condition (e.g., memory, cabling, switches. monitors etc.). GSM IT will manage the disposition of excess and surplus property IAW UCD PPM 350-80. Equipment is generally donated to the Campus Bargain Barn. In extremely rare cases, minimal proceeds from the sale of equipment through the UCD Bargain Barn are received and will be applied to the GSM IT operating budget. Equipment owners not willing to relinquish property to GSM IT will assume responsibility for processing their excess and surplus property IAW UCD PPM 350-80. Note: California Law and University Policy does not allow equipment to be transferred to public institutions outside of California or to any private entity.

Likewise, personal equipment cannot be donated to the school for disposal.

Printers, Paper, & Toner Cartridges

Purchasing local/desktop printers is strongly discouraged as it is very cost prohibitive. The GSM implemented a group printing solution as a strategic solution in 2008. Common use networked printers have been deployed at throughout the building. Individual printers for staff are no longer supported. Any remaining staff personal printers will be removed through attrition (i.e., when maintenance is required). Faculty are also encouraged to use, or migrate to, the common use printing solution. Faculty must fund any required service on all personal use printers.

Staff and faculty are responsible for purchase and replacement of toner cartridges and paper for all non-group printers. Staff/Faculty can re-order replacement toner cartridges via "UCD Buy" or can contact the GSM Business Office. It is preferred that original manufacturer (OEM) cartridges be ordered as opposed to remanufactured cartridges.

Specialized Applications/Systems

GSM IT recognizes that all computing support requirements will not be fulfilled by this Core Services SLA and that support for specialized applications needs to be addressed separately. A Service Level Agreement (SLA) will be developed for all specialized

applications/systems. The SLA will outline system requirements, financial responsibilities, and service expectations.

E-mail Delivery Problems

UC Davis provides e-mail services to all faculty, staff, students, and affiliates, but individuals have an option as to how their e-mail delivery is managed. Individuals choosing to have their e-mail forwarded to a 3rd party (off-campus) address (i.e., Gmail, MSN, etc) assume the risk of message delivery problems. Issues related to campus email services should be addressed directed with central IT. GSM IT staff are generally not provided necessary access to the campus email system necessary to effectively troubleshoot problems.

Training

GSM IT generally does not provide, coordinate, or fund training on computer systems or software. Staff/Faculty in need of training should consult with outside resources such as:

- UCD Staff Development and Professional Services
- UCD Arbor Faculty Center for Teaching and Technology
- UCD Summer Institute for Technology in Teaching (SITT)
- Off-Campus training conducted by third-party training providers

Training for specialized software systems used by the GSM should be developed and provided by the system sponsor (i.e., GSM unit that sponsored the deployment of the system/software).

GSM IT will provide individual orientation (approximately 30-60 minutes) to new staff/faculty on the GSM network/system operations (ref. Appendix E).

Research and Research Equipment

GSM IT does not have research assistants or adequate technical staff to offer programming and research support except when negotiated through specific service level agreement.

The GSM does not have adequate facilities to support research equipment and the UC IS-3 Cyber-Security policy introduces significant complexity for research equipment or any other shared computing systems. As such, the GSM promotes the use of AWS services to meet its research computing needs. Please discuss your needs with the Dean's Office and/or the GSM CIO/IT Director.

The GSM IT unit is responsible for the UC IS-3 Cyber-Security compliance reporting for the GSM. As such, it will be allowed full oversight of all computing/research equipment. Autonomous operations can be provided to Senate/Ladder Faculty, only if they identify themselves as an independent research center and accept all "Unit" level responsibilities

identified in the UC IS-3 Cyber-Security policy. In such cases, they will need to coordinate their activities with the campus Information Security Office (ISO) and be willing to accept all reporting/auditing requirements.

Instructional Equipment Preventive Maintenance

GSM IT performs regular preventive maintenance on classroom audio/visual equipment, student lab equipment, and student lounge equipment. Details of this preventive maintenance schedule is identified in a separate SLA developed for each instructional location (Gallagher Hall, UCDMC Education Building, San Ramon Bishop Ranch).

Loaner Equipment (including instructor equipment)

GSM IT does not possess loaner equipment for general purposes. A recommendation was provided to senior staff in June 2006 to purchase multi-media packages necessary to support their needs.

GSM Instructional Resources maintains minimal equipment for faculty use and GSM Student Affairs maintains minimal equipment for students. Please check with them if loaner equipment is needed.

By bargaining unit contract, NSF Unit 18 Instructors are to be provided access to information technology support that is reasonably necessary to complete their assigned duties and responsibilities. To that end, the following special provisions are provided for instructors:

> Instructors will be provided a loaner laptop, if requested, for their class

> Instructors will be provided reasonable personal equipment, if requested, from this list (or suitable alternative).

> Instructors will be provided up to two external monitors, if requested and if the GSM has requested they perform on-line or hybrid instruction (i.e., does not apply to "lecture recording").

Senate/Ladder Faculty must purchase any necessary equipment using their RATS.

VHS/DVD Cameras and other Audio/Visual Equipment

GSM IT does not possess VHS/DVD Cameras and other Audio/Visual Equipment. The Campus Academic Technology Services unit provides video services for the Campus and has the proper equipment to produce quality products. Use of their service is recommended. Information on their services is available at http://ats.ucdavis.edu.

Recording Lectures or Other Events

General support for videotaping lectures and/or other events is not a service generally supported by GSM IT (per GSM Faculty Support Model Workgroup (Jan 2007)). Individual faculty or event coordinators wishing to pursue such activities are encouraged to acquire services from Campus Academic Technology Services (ATS), commercial organizations, or rent equipment from ATS.

Exceptions have been made for special circumstances, such as the COVID pandemic. If teaching in a GSM classroom, please discuss your needs with the GSM PIRO/Instructional group. For lectures, please refer to the Loaner Equipment section above.

Student Computing Lab and Software

The GSM eliminated the student computing lab in 2010. Students must purchase/lease whatever software they need and install it on their personal laptops.

Remote Access

Allowing remote access to the GSM network can benefit staff and faculty by providing the flexibility to access system services from home or when on the road. However, providing remote access also introduces substantial risk since remote computers are often unmanaged and rarely Cyber-Safety compliant (ref: UCD PPM 310-22). To fully realize the benefits of remote access, this service must include robust, highly available, full-featured, and secure solutions that support the diverse user community with different connectivity and access requirements, including:

- Virtual Private Network (VPN) – remote connectivity to the campus network. Access can be acquired through the Campus VPN services (https://vpn.ucdavis.edu). Use of this service requires a Campus computing account. The user is responsible for ensuring remote computers are Cyber-Safety compliant.
- Secure Shell (SSH), Secure Copy (SCP), Remote Desktop Services (RDP), and Virtual Network Computer (VNC) are generally not allowed. Exceptions can be discussed based on business need.
- Email system. The GSM utilizes the campus uConnect email system, which employs Microsoft Office 365 email (i.e., cloud email service). Remote access to the email system will be provided through Microsoft's Office 365 system, a web accessible email client.
- GSM "MyOffice". The GSM provides access to various business applications through a web accessible Citrix application system. Access to this systems will require the user to install a Citrix web client software module.
- GSM Staff are provided AWS Workspaces as their primary computing environment, which allows direct remote access from any location.

Requests to setup a user for remote access will be considered low priority. Users should test their remote access prior to actual need.

Disaster Recovery and Data Backup

GSM IT will establish disaster recovery and data backup procedures for core network equipment. Backup procedures are for the sole purpose of disaster recovery from system failure and will not be used to support user error (i.e., accidentally deleted files, etc). Backup on desktop/laptop computers are the sole responsibility of the user.   Upon request, GSM IT will assist with establishing a backup protocol for desktop/laptop computers using Apple Time Capsule or Crashplan.com. The user is responsible for all costs associated with such implementations.

Domain Name Services

GSM IT will establish/renew registered domain names as requested. Registered names will be generally limited to the "gsm.ucdavis.edu" or "ucdavis.edu" domains. Commercial domain registration is possible, but functionality is extremely limited, so a specific service level agreement must be established.

Unsupported Services

Some of the service requests made to GSM IT may need to be resolved by other University departments or outside organizations. In these cases, GSM IT cannot guarantee the same level of responsiveness as described herein but will try to assist in providing a timely resolution of the issue. Examples of these situations include support for applications not developed or supported in-house (such as Kuali, Payroll, or Banner), and contracted services (such as printer repair).

GSM IT cannot support obsolete system. Systems are identified as obsolete and will become unsupportable when:

- The system is has not been replaced per the GSM standard replacement cycle (i.e., 4-5 years)
- hardware parts can no longer be obtained at a reasonable price
- hardware is incompatible with current technology
- software does not support current protocols or does not easily integrate with commonly used, current software versions.
- systems fall below minimum standards as defined by obsolete systems published at http://computerownership.ucdavis.edu.
- the operating system is more than two major releases behind
- GSM IT staff are not proxy-administrators for Campus computing accounts (i.e., Temporary Affiliate Form (TAF)), so cannot assist users in obtaining such accounts. GSM Instructional Resources is the designated GSM proxy-administrator for Campus computing accounts.

GSM IT does not support non-University owned hardware or software. If problems occur with personal equipment, GSM IT will be available for consultation on work-related questions, but will not fix any hardware or software problems.

GSM IT does not support the general maintenance of office business machines, for example fax machines, calculators, etc.

GSM IT does not generally support the following equipment unless a specific Service Level Agreement has been established:

- Any hardware or software that is <u>not</u> University-owned
- Telephones/Cell Phones
- Fax Machines
- Copy/Xerox Machines
- Other proprietary devices
- Obsolete equipment as identified above

GSM IT staff will *only* move computer equipment (<u>not</u> furniture, telephones, or other fixtures etc.) when users or offices are relocating within a reasonable proximity (e.g., in the same building). We will also disconnect and re-connect wiring components to ensure proper operation. Equipment move requests will be considered low priority. One to two weeks lead-time is generally considered best practice.

GSM IT staff do not provide technical support for special events. If technical support is desired for events, the cost of contracted services should be included in event planning.

Responsibilities of the Faculty/Staff/Students (i.e., Computer User)

All faculty/staff/students are expected to familiarize themselves with relevant UCD Policy & Procedure, including but not limited to UCD PPM, Section 310, Communications and Technology

All faculty/staff/students should familiarize themselves with available relevant documentation to enable effective use of information technology. They should also participate in relevant training to ensure that they have the necessary skills and understanding of technological tools.

All faculty/staff/students using audio/visual equipment should familiarize themselves with the equipment, including connections and operations. Additionally, portable audio/visual equipment should be tested prior to each scheduled presentation and any problems reported to the computer help desk.

Computer users should perform preliminary troubleshooting and information gathering prior to calling the IT Help Desk will help customers better describe their problem and help the IT staff resolve the issue more quickly. Relevant and helpful information includes: identifying the hardware and software being used, recording the error message

received, and identifying the printer name and location when a printer problem is encountered.

Supervisors should notify GSM IT of new hires and terminations within two (2) business days of an offer being extended or decision to terminate a person's employment. GSM IT will keep this information confidential when requested. This information is required for a variety of reasons, for example, maintenance of user accounts and listserv distribution list updates.

Users are responsible for un-installing software loaded onto home computers when appropriate – e.g., when finished using it, leaving the University, or transferring to another department/school.

Security is the responsibility of all computer users and users are cautioned not to share system logins and passwords.

It is against University policy to load any software from home (personal) onto University owned equipment.

Appendix A – Service Catalog

- Network Administration
  - Maintain and administer the core network infrastructure systems including authentication servers, file storage servers, data backup services, and print services.
  - Maintain email/calendaring services and setup accounts for permanent faculty/staff
  - Perform server installation & upgrades
  - Implement and monitor required system security
  - Coordinate administrative functions with Campus IT
  - Manage access security on network shares and files
  - Coordinate NAM activations
  - Establish and maintain departmental IT policy and procedures.
  - Audit and Investigative Services
    - Research
    - System Analysis
- Desktop Support to GSM Faculty and Staff *
  - Establish equipment standards and perform computer equipment purchasing
  - Maintain equipment and software inventory
  - Install hardware/software
  - Troubleshoot hardware/software problems and provide/arrange repair service as necessary.
  - Provide general technical advisory service
  - Perform preventive maintenance on workstations
  - Provide new user orientation on network navigation, basic e-mail/calendaring, application access, and computing policy & procedures
  - Provide system administration and Cyber-Safety reporting
- Desktop Support for GSM Students
  - Provide guidance on equipment standards
  - Provide general technical advisory service
- Information Systems
  - Develop and provide continued support for centralized development projects**
  - Implementation, custom development, and support of specialized applications**
  - Database Information System
    - Develop a centralized database information system
    - Develop/maintain user interfaces and reports*

* Note 1: Service limited to on-site at UCD (i.e., cannot provide service at faculty/staff residence) and limited to University owned equipment (i.e., not personal systems).

Appendix B – Standards & Conventions

Hardware

The GSM operates a managed network based upon Microsoft's proprietary Active Directory services. Minimal interoperability problems exist between Mac and PC systems, but computer users opting to use Apple equipment will need to accept some limitations. Known limitations include: Compatibility with Microsoft Exchange email/calendaring services, compatibility with the GSM print services, and compatibility with various software.

The GSM uses Microsoft's Active Directory services to reduce its cost of system administration and ensure compliance with campus cyber-safety policy. Cyber-safety compliance for computers not compatible with these services is the responsibility of the user.

Computer systems must support encryption using hardware Trusted Platform Module (TPM) that can securely store passwords, certificates, or encryption keys used to authenticate the system. All portable/laptop devices will be deployed with disk encryption enabled.

The campus has an agreement with Dell computers that provides significant discounts on Windows based desktop computers. The GSM IT will fully support Optiplex desktops and Latitude laptops purchased from Dell within its warranty period.

The GSM IT researches viable laptop alternatives on an annual basis. Current recommendations for non-Dell laptops include the HP Spectre 360 Pro.

Supported Apple equipment includes Mac Pro, iMac, Macbook, Macbook Pro, and iPads. GSM IT knowledge of Mac is limited, but every effort will be made to support Mac equipment as best possible.

The following software must be installed by the GSM IT unit on all computers:
- Sophos antivirus
- IBM BigFix Endpoint Management and Security agent

Computing equipment is generally supported for 4-5 years after purchase. The operating system version delivered with the computer at time of purchase will be supported. Operating system upgrades are generally not be supported, unless the upgrade is recommended by the GSM IT as part of a strategic business proposal.

Computer Authentication Services

Current UCD students, faculty, staff, and other UC Davis affiliates qualify for a UCD Computing Account. This account is required to access Campus services, such as Kuali, Campus e-mail, My UCDavis website, and various GSM websites. Everyone should register for a UC Davis Computing Account. Information about UCD Computing Accounts is available at http://computingaccounts.ucdavis.edu

GSM utilizes Microsoft Active Directory Services (AD) for its business network infrastructure. All Staff and Faculty will be provided a user account on the campus uConnect AD domain. Students will be provided a user account only if they are performing a function that requires such (normally not the case). An AD user account will provide access to core network services including access to secured business folders/files

All GSM hosted secure websites will be developed to use either the UC Davis Computing Account or database driven authentication services/functions as appropriate. All Students, faculty, and staff will be provided access as needed.

E-mail Services

UCD provides an e-mail account to everyone registering for a UCD Computing Account. This account should be sufficient for most students, temporary staff, and adjunct/visiting faculty/lecturers.

The GSM participates in the Campus uConnect Microsoft Exchange e-mail system that supports enterprise level e-mail/calendaring functions. An Exchange E-mail/Calendaring account will be provided to all permanent GSM faculty and staff. GSM IT recommends all permanent staff and faculty use the Exchange e-mail system as their primary e-mail system. GSM IT will recommend archiving practices for people that want to retain email that exceed designated capacity, but will not support archived email.

Group mailboxes for various business functions have been established on the campus Exchange e-mail system. Established distribution lists and mailboxes, including their assigned administrator (i.e., the person that keeps it up to date and ensures someone is assigned to review messages) are identified at http://support.gsm.ucdavis.edu/Shares/FAQs/GroupDistributionListsandMailboxes.pdf Anyone needing additional group distribution list should use the Campus "list" system. Information on this system is available at: http://lists.ucdavis.edu

Cell Phones

The GSM business office is responsible for phone service/equipment. Likewise, GSM IT does not provide spare/loaner equipment, does not repair phones/PDAs, and cannot provide service for non-University owned equipment. The extent of services simply includes providing guidance on standard connectivity mechanism supported by campus. If you are encountering problems with your device, we will provide minimal diagnostic evaluation and make every attempt to identify a reasonable action plan to satisfy your needs.

Database Services

GSM has a significant need for a central database repository for various applications and programs. Oracle databases are the de facto standard for large internet sites and enterprise applications and the UC system has a purchasing agreement with Oracle that offers substantial savings. Additionally, all primary business systems at UCD, including Banner, Kuali, and PPS, are currently hosted on Oracle platforms. As such, it is advantageous for information interchange and consolidation to utilize Oracle as the database services standard.

Appendix C – Supported Software List (cloud-services not included)

Vendor	Name	Version*
Microsoft	Windows O/S	Latest two major releases
Microsoft	Office & other productivity software	Latest
Apple	MacOSx	Latest two major releases
Adobe	All products	Latest
Sophos	Anti-Virus	Latest
DEA	EMS	Latest

* Note: Older versions are considered obsolete and are not supported. Newer versions will be supported upon production release.

Appendix E – Staff/Faculty Computing Orientation Topics

Computer Help Desk
- [ ] 752-4660 – We are here to help.
- [ ] IT Help Desk Hours 9:00AM – 5:00PM, Monday-Friday
- [ ] Use of Remote Assistance (Bombgar) – link to Computer Name (Service Tag #)

Network Overview
- [ ] Domains and User Accounts

Computer Security
- [ ] Log Off/Lock (Ctrl-Alt-Del) while away from desk and shutdown at night
- [ ] Use "Strong" passphrase
- [ ] Do not let anyone use your computer account and do not share password

E-mail
- [ ] E-mail clients (Outlook)
- [ ] Storage Limits
- [ ] Personal Folders (can create on local computer, but not supported by IT or backed up)
- [ ] Spam and setting up Rules
- [ ] Viruses and Attachments
- [ ] Outlook web-access (Office 365)
- [ ] Campus e-mail forwarding   http://computingaccounts.ucdavis.edu/

Remote Access
- [ ] MyOffice (office.gsm.ucdavis.edu)
- [ ] VPN (https://vpn.ucdavis.edu)

Data Storage and Backups
- [ ] C: Drive (not backed-up)
- [ ] Dropbox service (not backed-up)

Internet
- [ ] *Internet Browsers: Internet Explorer -or- Mozilla FireFox -or- Safari for Mac*
- [ ] GSM Home Page http://gsm.ucdavis.edu
- [ ] GSM Support Page http://support.gsm.ucdavis.edu

Printers
- [ ] Named by room location
- [ ] Adding Printers: START to RUN type \\Print\ (Right mouse click on printer Click connect)

Policies & Procedures (Please review the following important documents)
- [ ] UCD P&P, Section 310-23, Electronic Communications--Allowable Use
  http://manuals.ucdavis.edu/ppm/310/310-23.htm
- [ ] UCD P&P, Section 310-24, Electronic Communications--Privacy and Access
  http://manuals.ucdavis.edu/ppm/310/310-24.htm
- [ ] UCD Policy & Procedure, Section 250-05: Digital Millennium Copyright Act
  http://manuals.ucdavis.edu/ppm/250/250-05.htm
- [ ] UCD P&P, Section 310-22, UC Davis Cyber-Safety Program
  http://manuals.ucdavis.edu/ppm/310/310-22.htm

<u>Computing No-No's</u>

☐ **Please do not store sensitive information (e.g., name, SSN, driver id, financial info, security codes, etc) on computers.**

☐ Please do not use streaming audio or video

☐ Please do not open email attachments that are unexpected (beware of viruses)

☐ Please adhere to software licensing agreements