Service Partnership Agreement

Administrative Information Technology

Fiscal year 2018-2019

Table of Contents

GENERAL INFORMATION AND OBJECTIVES

Administrative Information Technology (IT) is a support unit serving the Finance, Operations & Administration (FOA) organization. IT's core mission is to provide comprehensive support for computers, business application systems, and other technologies. IT provides direct technical support to workstation and application users, indirect technical support through server and network administration, business-focused technology consulting, IT security and compliance management, and non-technical support through activities such as software licensing coordination, project support, and life-cycle management of IT assets. IT support encompasses fixed, mobile, and virtual devices; infrastructure and cloud services; data and database management; commercial software; and specialized line-of-business systems.

This Service Partnership Agreement (SPA) defines the manner in which IT will operate with transparency and accountability for services provided. In addition, this document outlines the roles and responsibilities for both the IT group and departmental business partners to support function-driven outcomes.

This document provides a service overview; for more detailed questions or concerns about anything written in this document, please reach out to the Client & Infrastructure Services Manager or your departmental Business Partner liaison.

1. SERVICE COMPONENTS

1.1 Service Area: Service Desk & Desktop Support

Administrative IT Services Provided

Administrative IT – Client Services provides an IT Service Desk and Desktop Support Services for more than 1800 clients throughout FOA, in more than 40 locations encompassing the UC Davis campus, City of Davis, and Sacramento. Services include software, hardware, and operating system support for client workstations (primarily laptop, desktop, and mobile devices). Throughout FOA, this support currently encompasses approximately 1650 workstations and their associated peripherals.

Normal service desk and desktop support hours are M – F, 7:30 am – 5 pm.

Most desktop support services are typically provided remotely, in order to minimize travel overhead and efficiently utilize limited staffing resources. In addition, on-site desktop support is provided as needed, subject to staffing availability. We also have scheduled on-site "office hours" in several locations, the details of which are published on our web site at https://adminit.ucdavis.edu/desktop-support.

Desktop support includes the following scope of services:

1) Manage Service Desk ticketing system
    a. Manage the life cycle of all desktop support requests.
    b. Triage and resolve incidents submitted by customers, escalating issues when necessary.

2) Manage IT hardware
    a. Provision and replace computer workstations and other IT equipment.

b. Replace workstations based on an IT-coordinated 3-year warranty and 4-year hardware replacement cycle.
c. Utilize a hardware deployment checklist to ensure consistent tracking, implementation and customer follow-up.
d. Maintain an inventory system to track the life cycle, cost, location, and status of workstations and related assets.

3) Manage network printers
   a. Acquire and deploy network printers.
   b. Create and administer network print queues.
   c. Coordinate with third party vendor for printer repairs.

4) Equipment loans
   a. Provide loaner devices (laptops, desktops, tablets) upon request for short-term use (subject to availability).
   b. Loans exceeding 30 days may require additional approval. For long-term (3+ months) or frequent recurring needs, departments should typically plan to acquire dedicated equipment.

5) Mobile phones and tablet devices (non-workstations)
   a. Coordinate purchasing and deployment of University-provided mobile devices.
   b. Obtain Portable Equipment Usage agreement signatures.
   c. Assist clients with configuring connection to UC Davis e-mail and collaboration tools.
   d. Assist clients with “Find Me” feature for cases of lost or stolen devices.

6) Software
   a. Manage automated and manual patches and upgrades to installed software.
   b. Support email and collaboration tools through the uConnect Cloud (Office365) service.
   c. Install and configure the following core software:
      i. Microsoft Office, Visio, and Project
      ii. Skype for Business (Microsoft Lync)
      iii. Adobe Acrobat (Reader or Pro, depending on client needs)
      iv. All three major web browsers: Internet Explorer/Edge, Firefox, Chrome
      v. Antivirus/anti-malware software
      vi. Support tools: BigFix, TeamViewer
   d. Install and configure non-core software by specific request:
      i. Adobe Creative Suite
      ii. Other software specific to the line of business needs for each department.
   e. Manage software license acquisition, renewals, and ongoing compliance for both core and non-core software.
   f. Software for supported workstations is purchased by AdminIT, but funded by business units with the following exceptions:
      i. Free software, such as the major web browsers
      ii. BigFix, TeamViewer

7) Security
   a. Manage workstations in compliance with requirements established by the UC Davis Cyber Safety Policy.

b. Scan workstations for Personally Identifiable Information (PII) on a periodic schedule, based on departmental data usage and associated risk.
c. Enable full workstation encryption, as applicable based on departmental requirements.
d. Administrative access to workstations is restricted to IT technicians unless required by business function. ***Exceptions require written approval by the requesting client's supervisor and the manager of Administrative IT – Client services.***
e. Provide guidance and tools for secure file transfers (e.g., Liquid Files)

8) Provide Data Storage
   a. Private "personal folder" network drive for each workstation user (typically the "H" drive).
   b. Limited access "group" network drive folders for business units (varies by unit needs). ***Note: individual workstations are not backed up, and should not be used for local data storage.***

9) Account Access
   a. Maintain updated user access lists for network resources, systems and tools.
   b. Facilitate the creation of Temporary Affiliate (TAF) and other computing accounts as needed.

10) Training
   a. Identify training and other client education resources for supported operating systems, software and tools, e.g., SharePoint, OneDrive, VPN, Office 365.
   b. Provide periodic email and web "Tech Tips".
   c. Provide written documentation.
   d. Provide links to online videos and tutorials.
   e. Provide personalized training per individual or team.

11) Surveys
   a. Provide support for the creation, tracking and reporting of online survey data.

12) Maintain FOA technology standards and guidelines documentation.

13) Provide ad-hoc consultation, analysis, and IT needs assessment.

14) Customer service feedback
   a. Provide periodic customer satisfaction surveys and other point-of-service mechanisms to enable continuous feedback and enhancement of services.

Business Partner Expectations

1) Service Requests
   - Submit routine service requests using the designated service management tool (ServiceNow):
     - Via web: http://adminit.ucdavis.edu – "Ask for Help" button
     - Via email: AdminIThelp@ucdavis.edu
   - Submit emergency service requests by calling 530-752-1222.
   - Respond to IT staff inquires in a professional and timely manner.
   - Notify IT staff in advance of scheduled actions and events with IT needs (e.g., new employee onboarding or requests to move computer equipment).

2) Data Management
   - Store data in appropriate locations (i.e., cloud, network file service and managed line-of-business systems, not end-user workstations or removable devices).
   - Designate departmental data stewards responsible for the following:
     - Specifying who should have access to departmental data and informing IT of any changes.
     - Identifying data subject to special handling, such as PII (personally identifiable information) and data covered by HIPAA, FERPA, etc.
     - Conducting PII reviews/remediation

3) Security
   - Comply with campus and departmental IT security policies and best practices.
   - Complete annual IT security awareness training.
   - Ensure physical security of devices (keep devices in attended areas or protected locked areas when not attended).
   - Request enhanced technical (Administrator) rights only where mandatory to perform university functions (i.e., "least privilege").
   - Do not bypass security practices (e.g., by using remote access workarounds).
   - Notify IT of suspected security breaches (e.g., compromised accounts/passwords, viruses, malware, etc.).

1.2 Service Area: System Administration

Administrative IT Services Provided

The System Administration service is responsible for the architecture, configuration, upkeep, security, and reliable operation of multi-user computer systems and other IT infrastructure components, such as servers, network storage, and firewalls. Throughout FOA, this support currently encompasses approximately 250 physical and virtual servers.

1) Business application services
   a. IT strategic planning and consultation.
   b. System architecture, solution design, and technical implementation.
   c. Application, database, and web hosting.
   d. System maintenance and support services.

2) IT liaison and vendor management
   a. Coordinate IT service delivery across multiple on- and off-campus providers.
   b. Assist business units with product and vendor selection.
   c. Align vendor efforts with business unit requirements, initiatives, and future plans.
   d. Securely manage appropriate vendor access to business systems.

3) IT infrastructure management
   a. Design, implement and maintain shared IT services and infrastructure, including compute, storage and networking resources
   b. Manage IT computing sites and IT colocation facilities.

c. Provide and administer virtual and physical servers.
d. Manage enterprise data storage (database and network file services).
f. Ensure security and IT policy compliance for managed systems and data.
g. Scan servers and other networked storage for Personally Identifiable Information (PII) on a periodic schedule, based on departmental data usage and associated risk.

4) Secure Network Connectivity
   a. Manage internet connectivity from the desktop to the campus network.
   b. Deploy, configure and maintain network firewalls.
   c. Provide secure remote access services, including terminal/remote servers (both general purpose and line-of-business) and Virtual Private Network (VPN).

5) System upgrades and customizations
   a. Provide analysis, recommendations, and support for system upgrades, testing and customizations.

6) Business continuity and disaster recovery
   a. Service monitoring, performance management and incident response.
   b. Application and data backup, recovery, and fail-over services.
   Note: individual user workstations are not backed up, and should not be used for local data storage.

The following lists the server uptime target. Please note that maintenance windows are excluded. The default maintenance window is the Sunday after the second Tuesday of the month from 12am – 6am.

Service Area	**Availability Target**
Server Availability	99% (i.e., two nines: yearly downtime of 3.65 days; monthly 7.20 hours; weekly 1.68 hours)

2. OPERATIONAL OBJECTIVES

The following sections describe response and resolution time targets based on ticket priority.

Response Time

Requestors using the designated service management tool (ServiceNow) will receive an immediate, automated email acknowledgement (typically within 5 minutes). During normal support hours, the target for assigning a ticket to a specific technician is fewer than or equal to **90** minutes. Ticket status can be reviewed by the requestor at any time via the Service Hub: https://ucdavisit.service-now.com/ess/incident_status.do

For critical or emergency issues, please call us at 530-752-1222.

Incident Resolution Time

The target time-to-resolve an *incident* ("Something is broken…") varies depending on the assigned priority.

Priority	Time-to-Resolve (workstation/individual)	Time-to-Resolve (departmental business system)
1 - Critical	<1 business day	1 business hour
2 - High	1-2 business days	4 business hours
3 - Moderate	2-5 business days	16 business hours
4 - Low	Up to 2 weeks	40 business hours
5- Planning	No specific target	No specific target

Priorities

IT is responsible for assigning ticket priorities. The table below summarizes the priorities currently in use.

Priority	Description	Example
1 - Critical	Incident - University Mission-Critical • Entire site loss or denial of service • Mission-critical core application not functional	• Central system infected by virus with rapid infection of desktops imminent
2 - High	Incident - Business Unit Critical • Department loss or denial of service • Business unit core application not functional	• Complete loss of departmental transaction database
3 - Moderate	Incident - Business Unit Process Efficiency • Department experiencing intermittent service or degradation in quality • Single critical user experiencing loss of functionality	• Location experiencing slow network performance, but still functional • Department head unable to access Wi-Fi
4 - Low	Incident - User Process Efficiency • Individual user experiencing problems	• Individual monitor has intermittent display issues.

Request Resolution Time

Service *requests* ("I want…") can also be assigned individual priorities, but they are usually categorized lower than *incidents*. Requests are resolved as quickly as possible given available resources and current incident load, and accounting for any necessary escalations or interactions with additional service providers. (For example, additional time may be needed to work with a vendor or approvers for IT purchase requests.) Section 5.3 lists some common IT requests and associated target resolution times.

3. OTHER PARTNER RESPONSIBILITIES

- Identify technology-related business needs, and engage with ADMINIT at the outset of any IT-related initiative (e.g., changes to line-of-business systems, development or purchase of new systems, etc.).
- Ensure staff receive training needed to effectively utilize both core productivity software (MS Office, email, web, etc.) and any departmental business applications, job-specific desktop software, and/or specialized IT hardware.
- Allocate appropriate funds to replace workstation hardware, and mobile devices, including tablets, on schedule: 3-4 years.
- Allocate appropriate funds to replace server hardware on schedule: 3-5 years.

4. CONTACT INFORMATION, SUPPORT HOURS AND ESCALATION

Information about submitting requests, normal business hours, and off-hours support is summarized below.

Contact Information

Phone: (530) 752-1222
Email: AdminIThelp@ucdavis.edu
Web: http://adminit.ucdavis.edu

Normal Support Hours

Monday – Friday
7:30 a.m. – 5:00 p.m.

After Hours Support

Administrative IT also provides after hours (24x7) call support for critical services, as identified in consultation with the Service Level Management Team.

Escalation

If you are not satisfied with the performance of the service or incident/request process, please contact one of the following individuals.	
Desktop Support Manager	Jerome Williams jnjwilliams@ucdavis.edu (530) 752-9063
Client & Infrastructure Services Manager	Jeff Barrett jtbarrett@ucdavis.edu (530) 752-9190
Admin IT Executive Director	Radhika Prabhu rprabhu@ucdavis.edu (530) 754-6805

5. SERVICE LEVEL MANAGEMENT

To understand how well IT is adhering to its customer service commitments, reporting and analysis will be conducted and shared with departmental Service Level Management Teams, typically comprised of the Admin IT Director, Client & Infrastructure Services Manager or Business Partner Liaison, Associate Vice Chancellor, and delegated business unit senior staff. The goal of service level management is to manage and improve the service provided to administrative units.

AdminIT agrees to meet established operational objectives. If AdminIT is unable to meet those requirements, additional resources may need to be identified or the relevant Service Level Management Team may be called upon to help with prioritization or resources procurement. It may be necessary to bring in senior AdminIT and administrative unit managers to change the priority of a support group in order to meet objectives. The goal is to provide the best possible service to customers.

5.1 Service Level Reporting

Depending on departmental needs, the following reports may be provided to the Service Level Management Team.

Report	Description
Desktop Support Metrics	Summarizes volume and type of desktop support incidents and requests, response and resolution times, and additional customer service metrics.
Server Uptime and System Administration Metrics	Provides the percent of availability for all production servers, along with additional systems administration service metrics.
Technology Roadmap Report	Summarizes scheduled work, new technology requests, completed requests, existing system/tools and retired/replaced systems/tools.
Disaster Recovery Report/Security Plan	Summarizes disaster recovery, business impact analysis, and security plan documentation and recommendations.
PII Report (Cyber Security compliance)	Lists storage locations of all detected PII data on servers and workstations in order to delete unused sensitive data, identify false positives and relocate PII to secure locations with protections, such as encryption.

Admin IT is responsible for facilitating reviews of this document. Contents of this document may be amended as required, provided agreement is obtained from the primary stakeholders and communicated to all affected parties.

5.2 Example Metrics

Specific service level metrics will include the following elements, typically measured at regular intervals and reported as trends:

Service Area	Metrics
Service Desk & Desktop Support	Number and categories of tickets submitted Ticket and workstation deployment backlogs Ticket response times Ticket resolution times Workstation breakdown by age & type
System Administration	Number and categories of tickets submitted Ticket backlog Ticket response times Ticket resolution times Production server availability/uptime

5.3 Additional Approaches for Measuring Customer Satisfaction

Administrative IT will provide multiple ways to measure customer satisfaction and client/partner perceptions. This data will provide insights into customer needs and level of satisfaction with interactions and service channels, providing an overall view of the partner engagement.

Outlined below are some additional approaches that will be utilized to measure IT performance:

- **Transactional or Caller Surveys**
  - IT will leverage service management tools to collect immediate feedback on the customer's experience.
  - Enables feedback for specific incidents, requests, and individuals.
  - Enables another view into IT training and performance monitoring.
- **Periodic Comprehensive Surveys**
  - IT will measure satisfaction across multiple service areas and dimensions to review ongoing service delivery.
  - Surveys will be created and distributed annually to review satisfaction from all customers.
  - This will provide valuable insight and awareness on internal IT interactions, as well as how IT works with partners and other customers.
- **Other Feedback Sources**
  - IT may create additional methods to log and measure immediate service concerns. An example might be a follow-up call after a service interaction.
  - This will allow IT leadership flexibility to detect and respond to issues or process problems not formally addressed in surveys.