

12/12/00  
Draft

# **Technology Handbook**

## **Performance Standards (SLAs)**

## **Table of Contents**

- I. Introduction
- II. Standard Services
- III. Production Service Level Requirements
- IV. Responsibility Matrix
- V. Escalation (Callout) List

## **Performance Standards (SLAs)**

### **I. Introduction**

SFA has Service Level Agreements (SLAs) with all its service providers. These SLAs define the performance standards that will be acceptable to the SFA. SLAs consist of 4 parts. They are:

- Standard Services
- Production Service Level Requirements
- Escalation (Callout) Lists
- Responsibility Matrix

These 4 parts of the SLAs are described in this document.

### **II. Standard Services**

There are standard sets of services that shall be provided by any service provider that enters into a Service Level Agreement (SLA) with the SFA. The following is the sample of Standard Mid-Range Services that are provided to the SFA:

#### **Standard Mid-Range Services**

- Primary data center operations and support services shall include:
  - Off line/Archive storage
  - System back up and disaster recovery services
  - Migration support (including the project plan)
  - System Database support
  - Change management control
  - Acceptance testing support; and

- Maintenance of GFI.
  
- Provide web hosting and operations support as follows:
  - Production Control
  - Console Operations;
  - Daily Production Support (24x7);
  - Workload Management;
  - Storage Tape Handling;
  - Problem Recognition, Diagnosis and Resolution;
  - System Programming/Utility Support;
  - Configuration Management;
  - DASD/Tape Management;
  - Data Security;
  - Disaster Recovery Coordination;
  - Documentation and Procedures;
  - Tape Library Maintenance; and
  - Contractor Network Management
  - Statistical Reporting of the web site

Any deviation from, or addition to this standard set of services is negotiated between the SFA and the Service provider, and written into the SLA. The following is an example of an addition to the Standard Mid-Range Services SLA that was negotiated between the SFA and the Service Provider.

## **Standard Mid-Range Services**

- System Availability Requirements:
  - Regular maintenance windows are NOT available (maintenance must be staggered across production servers)
  - Network ISP connectivity provided through high-capacity redundant lines.
  - Availability requirements effective within 6-months after migration.
  
- Planned maintenance windows
  - Present a justification to the ED-CIO for all scheduled maintenance– Preferred outage window - weekends, 5-7am (lowest volume)
  - Notify Apps Dev. 7 days in advance (to post outage notices)
  
- Help Desk Support
  - Provide Level 2 Help Desk support for data operations (level 1 will be provided by the applications developer)
  - Calls to Command Center answered in 4 rings by a support person
  
- Production meetings
  - Meet daily until web-site stability is achieved
  - Meet regularly, as needed, after the system is stabilized

## Standard Mid-Range Services

- Disaster Recovery (Production Only)

- Full production system capability shall be provided within 72 hours of a disastrous failure of Contractor's data center or any one of the production systems. (the applications developer shall support testing the restored production system functionality at the Contractor's designated disaster recovery site)
- Create a full system backup on the last business day of every week, including a full database export. Create incremental system backups at the end of every business day except those days that are the last business day of the week
- Documentation: Provide a description of the resumption of processing services in case of an adverse event. The plan shall specifically address disaster recovery for the production environment and must be consistent with the latest version of the Common Task Order disaster recovery plan to be provided.

- Government Furnished Items (if applicable)

- The Government plans to provide any required hardware upgrades and enhancements and system software licensing. The Government may, at its option, require the Contractor to provide these components.
- Prior to migration, ED shall provide to the Contractor a detailed list of all GFI (hardware, software and telecommunications) to be provided by the Government
- The Contractor shall provide maintenance coverage similar to or better than what is currently provided on all HW and system SW products

- Travel

- Required travel is a separate, reimbursable component of the task order - requires COTR approval prior to travel

### III. Production Service Level Requirements

SLAs for each system has unique features. The following defines the production service level requirements between SFA CIO and the Virtual Data Center (VDC) for Postsecondary Education Participants System (PEPS):

Targets are subject to a 3-6 month baseline

Performance Metrics are different from the SLA Metrics

SLA	SLA Metric	SLA Descriptors	Comments	Issues/Caveats
1) <b>System Platform Availability</b>	<ul style="list-style-type: none"> <li>99.3% of schedule availability by established time – Year 1</li> <li>99.4% of schedule availability by established time – Year 2</li> <li>99.5% of schedule availability by established time – Year 3</li> </ul>	<p><b>Descriptor:</b> Hardware and operating systems availability –server and all associated system software</p> <p><b>Availability:</b> Development server: 8x5 except Maintenance Window TBD</p> <p>Production server: 7x24 except Maintenance Window TBD</p> <p>Test Server: 8x5 except Maintenance Window TBD</p> <p>Stage server: 8x5 except Maintenance Window TBD</p> <p><b>Measurement:</b> (Total scheduled availability minutes – total outage minutes) / total scheduled availability minutes *100</p> <p><b>Exclusions:</b> Excludes Dept. of Educ. Approved/planned outages</p>	<p>Offering Based on:</p> <ul style="list-style-type: none"> <li>Technology</li> <li>Facilities infrastructure</li> <li>Operating systems</li> <li>Subsystem release levels</li> </ul>	99.5% unless engineered. Requires S request re
2) <b>Oracle Database and Application Availability</b>	<ul style="list-style-type: none"> <li>99.3% of schedule availability by established time – Year 1</li> <li>99.4% of schedule availability by established time –</li> </ul>	<p><b>Descriptor:</b> Availability of Oracle PEPS application software, including forms server, web server, concurrent manager, database, etc.</p>		99.5% unless engineered. Requires S request re

	<p>Year 2</p> <ul style="list-style-type: none"><li>• 99.5% of schedule availability by established time – Year 3</li></ul>	<p><b>Availability:</b> Production database: Monday-Friday 8am-8pm EST</p> <p><b>Measurement:</b> (Total scheduled availability minutes – total outage minutes) / total scheduled availability minutes *100</p>		
--	---	---	--	--

SLA	SLA Metric	SLA Descriptors	Comments	Issues/Caveats
3)	<ul style="list-style-type: none"> <li>•</li> </ul>	<b>Exclusions:</b> Excludes Dept. of Education Approved /planned outages	<ul style="list-style-type: none"> <li>•</li> </ul>	
4) <b>EAPP Production Web Server Response Time</b>	<ul style="list-style-type: none"> <li>• Average Internal Response time &lt;= 3 seconds</li> </ul>	<b>Descriptor:</b> Less than 3 seconds avg. internal response  <b>Measurement:</b> Total response time for included transactions during measurement period/ total # of included transactions for measurement period  <b>Exclusions:</b> <ul style="list-style-type: none"> <li>• System Transactions</li> <li>• File transfer transactions</li> <li>• Transactions using &gt;= 3 seconds of CPU</li> <li>• Development, Test, QA Environments</li> <li>• Print Transactions</li> <li>• Background Transactions</li> </ul>	<ul style="list-style-type: none"> <li>• This target is subject to a 3-6 month baseline</li> </ul>	Users should not have more than 25 file transactions per day.  Need to verify existing transactions provide this measurement. Measurements are not included in cost model.
5) <b>VDC Internet Availability</b>	<ul style="list-style-type: none"> <li>• 99.6% of schedule availability by established time – Year 1</li> <li>• 99.7% of schedule availability by established time – Year 2</li> <li>• 99.8% of schedule availability by established time – Year 3</li> </ul>	<b>Descriptor:</b> Availability of Web Server via Internet  <b>Availability:</b> Monday-Friday 6am-10pm  <b>Measurement:</b> (Total scheduled availability minutes – total outage minutes) / total scheduled availability minutes *100  <b>Exclusions:</b> Excludes Dept. of Educ. Approved /planned outages	<ul style="list-style-type: none"> <li>• This target is subject to a 3-6 month baseline</li> </ul>	

SLA	SLA Metric	SLA Descriptors	Comments	Issues/Caveats
6) Citrix Server availability	<ul style="list-style-type: none"> <li>99.3% of schedule availability by established time – Year 1</li> <li>99.4% of schedule availability by established time – Year 2</li> <li>99.5% of schedule availability by established time – Year 3</li> </ul>	<p><b>Descriptor:</b> Availability of Web Server via Internet</p> <p><b>Availability:</b> Monday-Friday 6am-10pm</p> <p><b>Measurement:</b> (Total scheduled availability minutes – total outage minutes) / total scheduled availability minutes *100</p> <p><b>Exclusions:</b> Excludes Dept. of Educ. Approved /planned outages.</p>	<ul style="list-style-type: none"> <li>This target is subject to a 3-6 month baseline</li> </ul>	
7) Help Desk	<ul style="list-style-type: none"> <li>All calls answered within 30 seconds</li> <li>Abandon rate 5% or less</li> <li>1<sup>st</sup> call resolution 80%</li> </ul>	<p><b>Measurement:</b> ACD statistics used to measure length of time to answer calls and to calculate abandon rate. Problem tracking system used to calculate 1<sup>st</sup> call resolution.</p>		
8) Backups	<ul style="list-style-type: none"> <li>As Scheduled</li> </ul>	<p><b>Descriptor:</b> Backups of Oracle application/systems software and data will be performed nightly</p>		
9) User Registration Requests	<ul style="list-style-type: none"> <li>Within 48 hours of receipt of approved requests</li> </ul>	<p><b>Descriptor:</b> Within 48 hours of receipt by IT Services assumes request form is properly completed including approval signatures.</p>		

**Notes:**

- 1) Each SLA has an owner (Line of Service). This SLA owner is responsible for identifying and installing (as necessary) the appropriate monitoring and capturing tools
- 2) The process of how the SLA metrics are reported on to Acct. Mgmt. (by the LoS) and the client (by the Acct. Mgmt) needs to be identified.
- 3) There are no penalties associated with this SLA.
- 4) CSC will provide a Root Cause Analysis report for all outages. This root cause analysis report will be used to determine which SLA receives the hit for an outage.  
Outages that affect system availability will be charged against the SLA that is closest to the root cause. A missed SLA will not cascade to others.  
If a miss occurs on system availability, a miss will not be recorded for Oracle Availability, WWW Availability, WWW Response Time.
- 5) Critical Batch Processing Completion and Critical Batch Output Delivery are not required at this time.

**IV. Responsibility Matrix**

Service Level Agreements (SLA) between the SFA and the Service Providers also contain a Responsibility Matrix. This Responsibility Matrix defines all the tasks that are to be performed under this SLA, and assigns primary responsibility for the performance of these tasks. The following pages contain a sample Responsibility Matrix.

Task No.	TASK DESCRIPTION	RESPONSIBLE ORGANIZATION				P = Primary
		SFA Business Unit	CBS Development	SFA/CIO IT Services	VDC	
	<b>Requirements, Capacity Planning and Recommendations</b>					A = Appr
1	Submit Hardware and Software Requirements for CBS to SFA/CIO.	A	P			S = Supp
2	Submit project plan/schedule that identifies support services needed to SFA/CIO and CSC.	A	P		S	J = Joint
3	Submit CBS recommendations to SFA/CIO.	A	P			
4	Submit project plan/schedule to SFA/CIO.	A	P			
5	Initiate and track all HW and SW and requested services as outlined in project/schedule plan, and share with CBS team and CSC.				P	
6	Perform technical reviews of hardware changes and coordinate the installation or deinstallation of hardware. Ensure the appropriate facilities (floor space, power, air conditioning) are available.				P	
7	Notify SFA/CIO of all expected HW/SW deliveries				P	
	<b>Installation Setup and Systems Configuration for Development and Production Environments</b>					
8	Receive and configure hardware and network purchased by SFA/CIO.				P	
9	Installation and Configuration of Operating System				P	
9a	Install application and database software installation in conjunction with CSC.					
10	Installation and Configuration of System Utilities				P	
11	Installation and Configuration of Network & Communication Infrastructure				P	
12	Installation and Configuration of Backup Facility				P	
13	Installation and Configuration of Security System				P	
	<b>Applications Administration and Management</b>					
14	Identify staffing requirements	A		J		J
15	Identify staff training requirements necessary to perform job duties	A		J		J

17	Provide IP source/destination information for application developer requiring access to the CBS system (to initiate security authorization process). Identify specific protocols required.						
18	Provide CSC with IP source/destination information to authorize access for the specified application developer				P		
19	Set up remote administration capabilities for authorized users					P	
20	Responsible for database software upgrades.	N/A	N/A	N/A	N/A	N/A	
21	Configure Application software			P			
22	Deploy application software			P			
23	Monitor and analyze IIS logs			P		S	
24	Provide Application Statistics			P		S	
25	Provide application support for users during development.			P			
25a	Resolve user id and password problems, create & delete user ids as required (within the context of the business area or application).						
27a	Respond to user feedback	P		S			
27b	Implementation of changes and/or corrections as needed	A		P			
28a	Develop trouble-shooting procedures to respond to application			P			
	<b>Performance Management and Reliability</b>						
29	Perform regular server maintenance					P	
30	Notify designated contacts on any scheduled downtime for upgrades and/or maintenance.					P	
31	Develop trouble-shooting procedures to respond to server/communications problems						
32	Identify and recommend tools (testing, monitoring, scheduling, etc.)					P	
33	Utilize a tracking system for problem reports and problem resolution	J	J	J	J	J	
34	Perform technical reviews of software changes and coordinate the installation or deinstallation of software i.e. patches, PTFs		S	S		P	
35	Responsible for providing support for internal and external audits.	J		J	A	J	
36a	Responsible for generating monthly system performance report for the production servers to include CPU Utilization, Disk Activity, Network Utilization, and Memory Utilization.						

36b	Responsible for generating monthly application performance report including problem calls, bug fixes, etc.			
37a	Identify and implement any short-term fixes to eliminate the immediate system problems.			
37b	Identify and implement any short-term fixes to eliminate the immediate application problems.			
38a	A permanent, corrective action will be identified and implemented with appropriate follow-up to ensure the fault is eliminated from the application.			
38b	A permanent, corrective action will be identified and implemented with appropriate follow-up to ensure the fault is eliminated from the application.			
39	The problem will be documented and tracked by the respective contractors' problem management process.			P
	<b>COMPUTER OPERATIONS</b>			
40	Follow all appropriate Change Management, Problem Resolution & Escalation Procedures.	J		J
41	Document and report hardware and software problems following the troubleshooting and escalation procedures.			P
42	Provide 24 x 7 system level support of CBS production and development systems (if required).			
43	Monitor computer room environment and ensure that the systems are operational.			
44	Provide removable tape support to include: mounts, tracking, onsite, off-site storage, tape purchasing, shipping and receiving.			
45	Provide an immediate response to unplanned events by identifying, escalating, and documenting the problem.			
46	Coordinate hardware issues with appropriate vendors.			P
47	Update procedures and documentation accordingly.			P
48	Provide Single Point of Contact (Command Center) for Network and Server Operations.			

49	Provide a Single Point of Contact (Service Delivery Manager) for business issues and service levels.						
50	Schedule/monitor CA-Unicenter batch processing.	N/A	N/A	N/A	N/A	N/A	
51	Maintain CA-Unicenter Calendars.	N/A	N/A	N/A	N/A	N/A	
52	Maintain CA-Unicenter Event Management Definitions.	N/A	N/A	N/A	N/A	N/A	
53	Maintain CA-Unicenter Job and Jobset Definitions. Update and distribute definition spreadsheets as changes are made.	N/A	N/A	N/A	N/A	N/A	
54	Perform abend resolution.	N/A	N/A	N/A	N/A	N/A	
55	Restart jobs once abort has been resolved.	N/A	N/A	N/A	N/A	N/A	
56	Create morning report with processing statistics for numbers of records processed and abort log.	N/A	N/A	N/A	N/A	N/A	
57	Distribute Morning report statistics	N/A	N/A	N/A	N/A	N/A	
58	Respond to system and network outages, application unavailability, hardware failures, and inquiries concerning problem status.			S			P
59	Reporting for system and network outages, application unavailability, hardware failures, and inquiries concerning problem status to be passed out during Daily Turnover Meeting			S			P
	<b>SECURITY</b>						
60	Disseminate privacy-related information that may affect OSFA related systems					P	
61	Perform regular penetration testing of the systems and provide documentation of results to the CBS POC.						P
62	Stay current with OSFA security regulations and guidelines	J	J	J	J	J	
63	Provide the processes and activities needed to create, modify, and delete Logon IDs.						
64	Create user groups and security levels for user logins.						P
65	Maintain User IDs and passwords. The System Security Officer will provide authorization for users, and CSC will create and delete users as needed.						
66	Utilize CA-Unicenter, The Next Generation (TNG), to implement security on the development and productions UNIX servers.	N/A	N/A	N/A	N/A	N/A	

67	Provide any additional security requirements/guidelines to be met.	S			P	
68	Provide adequate resources (such as space, CPU, memory) to run security tool for application security.					
69	Provide reports on unauthorized and or unsuccessful attempts to access the system.					
70	Review security reports and take appropriate action(s) to ensure CBS assets are adequately protected.	A		S		P
71	Review industry security alerts and determine appropriate course of action.			J	J	J
72	Recommend security enhancements.			J	J	J
73	Verify Login IDs have not been used before.					P
74	Determine security clearance level for employees, contractors and subcontractors associated with the Internet					
75	Provide a single point of contact for all security related issues.			J	J	J
	<b>SYSTEMS ADMINISTRATION</b>					
76	Inventory and track system-level software components (such as the operating system and other non-application software) that make up the Midrange platform environment.					
77	Provide inventory information to the U.S. Department of Education.					P
78	Perform preventative maintenance according to supplier recommendations and based on the stability of the Midrange platform environment.					
79	Responsible for evaluating, installing, and testing software fixes provided by Hardware Provider in accordance with the change management procedures.					
80	Responsible for installing and resolving failures for system-level or non-application software.					
81	Responsible for reviewing supplier product status and maintenance information of system-level software to identify current version information and known potential problems.					
82	Responsible for the back-up and recovery of system-level data (such as the operating system and other non-application data stored on the system).					

83	Renew and maintain software licenses for system-level software.					P	
84	Renew & maintain hardware and software maintenance agreements					P	
	<b>DISASTER RECOVERY</b>						
85	Responsible for restoring computer operations and the operating environments, both at the recovery location and at the old, repaired, or reconstructed data center site.						
86	Responsible for ensuring that all users and clients are familiar with the Disaster Recovery Plan and interface with users and clients during a disaster.	P				S	
87	Responsible for restoring voice and data telecommunications links between VDC and the CBS locations.						
88	Responsible for restoring all designated critical applications.			P			
89	Responsible for reestablishing the tape library function at the primary site or at the alternate processing site.						
90	Responsible for restoring the operating environment at the primary site or at the alternate processing site.						
91	Create and maintain emergency contacts list.	J		J	J	J	
92	Escalate to designated personnel in the event of a disaster.	S				P	
	<b>CHANGE MANAGEMENT PROCEDURES</b>						
93	Responsible for all system modifications of directories, security on directories, and access privileges to the servers. Remove security on directories, and access privileges to the servers.						
94	CBS application contractor requests change and provides necessary information (request name, date & time of change, change procedure backout plan, risk assessment, contact name) in written form so that VDC can complete the request.		S	P			
95	Application contractor sends request to the VDC representative for completion.			P			

96	The VDC representative will input change into the VDC change management system and notify appropriate parties.				
97a	The VDC personnel will be responsible for implementing the system change, which includes testing and documentation of all activities for implementing the change.				P
97b	The VDC personnel will be responsible for implementing the applications change, which includes testing and documentation of all activities for implementing the change.	S	S		P
98	The VDC personnel will complete the change and notify the VDC representative that the change has been completed.				
99	The VDC representative will notify the Application contractor that the change has been completed.				
	<b>NETWORK SECURITY</b>				
100	Maintain Network capacity to meet or exceed the Systems Operation Times and Required Availability as outlined in ED standards documents, such as the Project EASI-ED Program System-Wide Standards Document and SFA Modernization Blueprint.				
101	Determine protocols and sufficient address ranges				P
102	Obtain and implement Virtual Data Center (VDC) Network access permissions from OSFA.				
103	Configure and operate *VDC Network Equipment (Routers, Firewalls, etc). to enforce OSFA security rules.				
104	Configure and operate **Application Vendor Network Equipment (Routers, Firewalls, etc.). to enforce OSFA security rules.				
105	Monitor VDC Network Equipment for evidence of security violations / violation attempts.				
106	Monitor Application Vendor Network Equipment for evidence of security violations / violation attempts.				
107	Support VDC penetration testing efforts commissioned by the OSFA.				P
	<b>DATABASE</b>				

108	Recommend/select the most appropriate DBMS for development or modification of an application.	N/A	N/A	N/A	N/A	N/A	
109	Participate in the configuration of the DBMS on the runtime platform.	N/A	N/A	N/A	N/A	N/A	
110	Work with the Infrastructure team to install the DBMS and subsequent vendor releases and PTF's.	N/A	N/A	N/A	N/A	N/A	
111	Participate in and approve the application database design, to include:	N/A	N/A	N/A	N/A	N/A	
	Assistance in determining data requirements, data relationships, and logical design	N/A	N/A	N/A	N/A	N/A	
	Design of physical structures	N/A	N/A	N/A	N/A	N/A	
	Consulting on the naming and definition of data elements	N/A	N/A	N/A	N/A	N/A	
112	Create the database instance, name, establish directory structures, and allocate database files.	N/A	N/A	N/A	N/A	N/A	
113a	Allocate databases and tablespaces based on the identified needs of the application and anticipated data growth.	N/A	N/A	N/A	N/A	N/A	
113b	Create scripts in the development environment for the creation of databases by the VDC	N/A	N/A	N/A	N/A	N/A	
114	Create/alter database objects, including creation of tables, indexes, views, triggers, stored procedures, packages, sequences, synonyms, table constraints.	N/A	N/A	N/A	N/A	N/A	
115	Work with the Security team to administer database access, including tasks such as:	N/A	N/A	N/A	N/A	N/A	
	create/enable roles or groups	N/A	N/A	N/A	N/A	N/A	
	grant permissions	N/A	N/A	N/A	N/A	N/A	
	assign default database/tablespaces	N/A	N/A	N/A	N/A	N/A	
	assign default roles or groups	N/A	N/A	N/A	N/A	N/A	
	set profiles and quotas	N/A	N/A	N/A	N/A	N/A	
	authorize user connections	N/A	N/A	N/A	N/A	N/A	
116	Coordinate production database deployment, including tasks such as:	N/A	N/A	N/A	N/A	N/A	
	moving files to production directories	N/A	N/A	N/A	N/A	N/A	
	compiling stored procedures and triggers	N/A	N/A	N/A	N/A	N/A	
	creating scripts for backups/loads/unloads	N/A	N/A	N/A	N/A	N/A	

117	Determine/implement appropriate database backup strategy, including decisions regarding database data files, control files, redo log files, transaction logs, export/import, dumps, and image copies.	N/A	N/A	N/A	N/A	N/A	
118	Perform production database recovery when necessary (e.g., perform recovery/restore from backup data files and redo logs/transaction logs when the recovery cannot be handled by operational staff).	N/A	N/A	N/A	N/A	N/A	
119	Monitor and tune databases, including reallocating space as needed, determining archive process, and reorganizing databases as needed.	N/A	N/A	N/A	N/A	N/A	
120	Provide database design and call pattern reviews as required for in-house developed applications and COTS packages.	N/A	N/A	N/A	N/A	N/A	
121	Perform database problem tracking and resolution.	N/A	N/A	N/A	N/A	N/A	
122	Review and recommend DBMS tools needed to manage the database environment.	N/A	N/A	N/A	N/A	N/A	
123	Recommend DBMS standards and guidelines for database design and data access.	N/A	N/A	N/A	N/A	N/A	

**V. Escalation (Callout) List**

Every Service Level Agreement provides an Escalation (Callout) List. This list defines all potential problems that could occur in the provision of the Services defined in the SLA. This list also contains the names and phone numbers of personnel to be called, when these problems do occur. The following pages contain a sample of the Callout List.

CAMPUS-BASED/SFA Callout list

**Hardware:** HP

**H/W Maintenance Coverage:** 7 x 24

VDC Operations				
Function	Name	Office #	Beeper #	Pin #
<b>Operations Primary</b>	Command Center	203-317-5051 24 hrs x 7 days	N/A	N/A
<b>Operations Secondary</b>	Shift Leader	###-###-####	N/A	N/A
<b>Operations Third</b>	Name	###-###-####		
<b>Operations Primary Manager</b>	Name			
<b>Operations Backup Manager</b>	Name			N/A
<b>Account Executive</b>	Name			

VDC System Problems				
Function	Name	Office #	Beeper #	Pin #
<b>System Admin., Primary</b>	Command Center		N/A	N/A
<b>System Admin., Secondary</b>	Name			N/A
<b>System Admin., Third</b>	Name			
<b>System Admin., Primary Manager</b>	Name			
<b>System Admin., Backup Manager</b>	Name			N/A
<b>SFA Admin.. Primary Manager</b>	Name			N/A
<b>SFA Admin.. Secondary Manager</b>	Name			N/A

VDC Communications Problems				
Function	Name	Office #	Beeper #	Pin #
<b>Network Services, primary</b>	Network Services On-Call Pager			
<b>Network Services, secondary</b>	Name			

CAMPUS-BASED SYSTEM				
Function	Name	Office #	Beeper #	Pin #
<b>Application Primary</b>	Name			N/A
<b>Application Secondary</b>	Name			N/A
<b>Application Third</b>	N/A			N/A
<b>Application Primary Manager</b>	Name			N/A
<b>Application Backup Manager</b>	N/A			N/A
<b>Application Backup Manager</b>	N/A			N/A

CAMPUS-BASED Database Problem				
Function	Name	Office #	Beeper #	Pin #
<b>CB/SFA Database Admin Primary</b>	Name			N/A
<b>CB/SFA Database Admin Secondary</b>	Name			N/A
<b>CB/SFA Database Primary Manager</b>	Name			N/A

12/12/00  
Draft

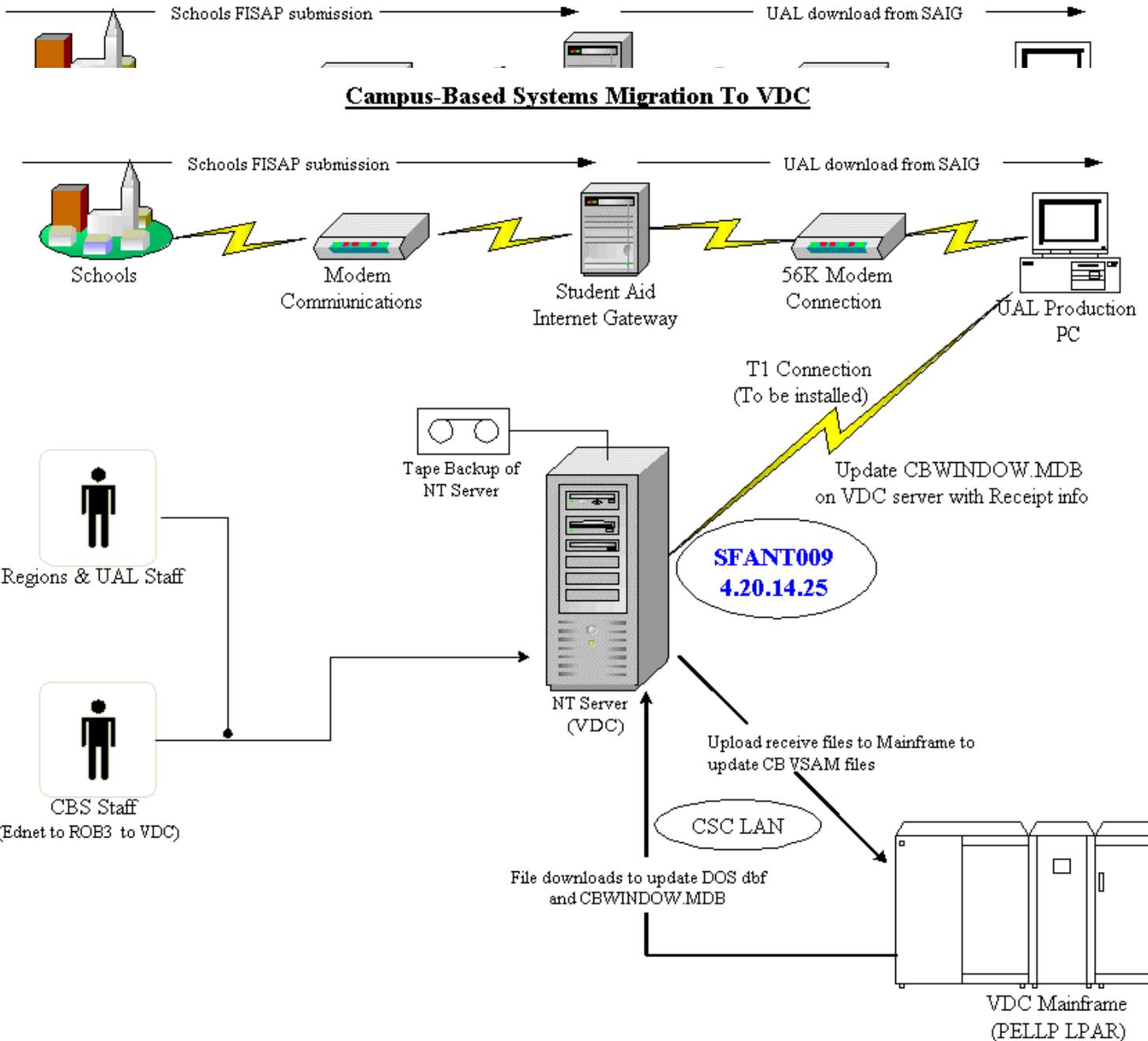
Service level Agreements also provide procedures for troubleshooting problems that occur in the provision of the service by the service provider. The following is a sample of Troubleshooting procedures for a system at SFA:

### **CAMPUS-BASED System (CBS) Troubleshooting Procedures**

CBS is comprised of:

See attached diagram

## Campus-Based Systems Migration To VDC



### **Procedures for ED Staff and Contractors**

In the event that the Campus-Based System goes down, use the following set of procedures to alert Contractor staff and resolve the problem.

1. Call the VDC Command Center at 203-317-5051. Someone is onsite 24 x7.
2. The person who answers the phone will be one of the operations staff.
3. Tell the operations staff that you are calling about an OSFA system and provide the name of the system, its IP address, if known and as complete a description of the problem as possible.
4. The operations staff will contact the system administrator on call for the system in question.
5. The system administrator will call you back if additional information is needed.
6. The system administrator will troubleshoot the system. If they are able to troubleshoot the system without a system reboot, they will resolve the problem and report back.
7. If the problem requires procedures that need our authorization, they will report back with their recommendation on what needs to be done. We can then look at the system and make our own determination, or accept the recommendation from the contractor system administrator.
8. If a reboot is necessary, OSFA needs to give the system administrator authority to proceed with the system reboot.

12/12/00  
Draft

9. The VDC may decide to convene a bridge call to bring other parties into the problem resolution process.

### CBS Contact List

Order in which ED Staff and Contractors should be called in the event that the VDC detects a problem with the CBS server.

Danny Dytang	ED	CBS Contractor - UAL	301-565-0032			
Harrison Bannister	ED	CBS Computer Spec.	202-708-5776	301/262-7393		
David Elliott	ED	OCIO Rep	202-401-0551	202/257-5071		
James Cunningham	ED	OCIO Rep	202-708-8188			
Phillip Wynn	ED	OCIO Rep	202-260-0080			

12/12/00  
Draft

## Virtual Data Center Contacts

- Call the Command Center at 203-317-5051 and work with the System Administrator on duty

Name	Title	Function	Email	Phone	
Jerry Ryznar	Account Manager	Oversees contract	grvznr@csc.com	301-794-6374	
Dave Lass	Service Delivery Manager	Oversees all aspects of delivering service	dlass@csc.com	203-317-5037	
Fariba Aliloo	Server Manager		faliloo@csc.com	203-317-5047	
Dan Wagner	Project Manager		dwagner5@csc.com	203-317-4830	
Dave Murdy	Systems Admin		dmurdy@csc.com	203-317-4818	
Tim Cronin	Systems Admin			203-317-5025	
Bob Chatman	Systems Admin		rchatman@csc.com	203-317-2130	
Dave Hugh	Network Manager		dhugh@csc.com	203-317-5006	
Mo Asheh	Network Admin		masheh@csc.com	203-317-5187	
Jim Rotchford	Security Coordinator	OSFA security	jrotchfo@csc.com	203-317-5007	
Ben Smith	Operations Manager	ED operations	bsmith1@csc.com	203-317-2178	
Rich Ryan	Oracle DBA	Norwich	rryan@csc.com	860-701-1209	