

SFA Modernization Program
United States Department of Education
Student Financial Assistance



VDC Transition Plan

Task Order #22
Deliverable #22.1.2

October 23, 2000

Table of Contents

Overview	3
Summary of Required Documents	4
Installation Checklist	4
Production Support Matrix	4
Physical and Logical Diagram	4
Escalation List	5
Responsibility Matrix	5
Due Diligence Checklist	5
Troubleshooting Document	7
Memorandum of Understanding	7
Run Book	7
Other Useful Documents	8
Port Identification Form	8
Hardware and Software Planning Template	8
Operations Readiness Checklist	8
Change Request Form	9
New Services Work Order Form	9
Overview of Access Security Clearance, SFA IT Systems	10
Summary of Forms Needed by Risk for Contractor Employees	13
Summary of Form Descriptions and Usage	14
Procedure to obtain EDLAN network access	16
Procedure to obtain EDNet Clearances	17
Employee Security Tracking Sheet	18
See Appendix O for Samples of Security Forms	19
Procedure to Obtain VDC Access and Access to Other Applications	20
Appendices	

Overview

This document outlines the documents that the VDC currently requires in order to accept an application for production operations. Also included in this document is an explanation of the process and forms required to gain access to the systems at the VDC and to obtain an EDLAN account. It is recommended that applications consider providing similar documentation for development systems in order to ensure the stability of those systems. However, service level agreements are not currently maintained on development systems by the VDC.

This list was compiled based on the experiences of installing the technical architecture components of the first several modernized applications in the virtual data center (VDC), in particular, the FMS, Schools Portal, and IFAP projects. It is important to recognize the processes and examples included in this deliverable were documented as they were perceived by project teams, not as they should be done permanently.

There are no documented guidelines by the VDC on lead times for preparing and submitting these documents. The critical requirement is that they be done prior to production. It is important to work closely with the VDC staff as the project takes place to ensure documentation is prepared, reviewed and accepted by all parties involved in conjunction with the production readiness target dates.

The initial section of this document describes each form that is required by the virtual data center to become a production application. The next section describes some additional documents that are very useful during development. Also included in this document is a description of the process to obtain security clearance for contractors as it has been perceived by our project teams. Incorporated at the end of this document are appendices with a sample of each of the forms listed throughout this deliverable.

Summary of Required Documents

This section describes the purpose and method of completion for each of the required documents for an application to go into production at the virtual data center. The location of a sample of each one of these documents is given at the end of each description.

Installation Checklist

Purpose: For use in performing a complete system reinstall if required.

Method of Completion: This document should be created during the initial system installation in the production environment. All adjustments and changes that occur after installation should be documented and the installation instructions updated accordingly. Installation in the production area should follow the procedures created in order to verify that the instructions are accurate.

Tips: This is a living document. It should be reviewed at the time of new releases to determine whether any changes are required. It would also be prudent to periodically test the instructions as part of a system recover test plan.

See Appendix A

Production Support Matrix

Purpose: This document is used by Operations Staff at the VDC to contact the appropriate technical support staff in the event system failure or problems occur. All technical support groups should appear here, including VDC personnel. This is also known as the Callout List.

Method of Completion: The VDC will complete the section relating to the VDC contact numbers. Unless the system availability is planned only for normal business hours, this document must include phone numbers for off-hours. These can be home phone numbers, cell phones, beepers, or all three. The names should be listed in the order in which they should be contacted. If the first individual cannot be reached, or cannot resolve the problem, the next person on the list will be contacted. The number of names listed is entirely up to the project, but there should be more than two for each area.

Tips: This is a living document. It should be reviewed periodically and at the time of new releases to determine whether any changes are required.

See Appendix B

Physical and Logical Diagram

Purpose: This document is used by Operations Staff at the VDC, applications maintenance staff, and business units to provide all parties with a common frame of reference.

Method of Completion: The Technical Architecture team can provide assistance with creating the physical diagram, and the VDC does not require network configuration information. The diagram should show relationships and dependencies between all products and other systems.

Tips: This is a living document. It should be reviewed periodically and at the time of new releases to determine whether any changes are required.

See Appendix C

Escalation List

Purpose: To provide instructions for the Application Support team or the Business Area to contact the VDC in the event of a problem. In addition, it lists the business managers in the event some activity impacting service delivery to the public must be planned or implemented (such as unscheduled down time) and the VDC management team in the event the Application Support team or the Business Area feel they need to escalate an issue within the CSC management team.

Method of Completion: The VDC will complete the section relating to the VDC contact numbers. Unless the system availability is planned only for normal business hours, this document must include phone numbers for off-hours. These can be home phone numbers, cell phones, beepers, or all three. The names should be listed in the order in which they should be contacted. If the first individual cannot be reached, the next person on the list will be contacted. The number of names listed is entirely up to the project, but there should be more than 2 for each area.

Tips: This is a living document. It should be reviewed periodically and at the time of new releases to determine whether any changes are required.

See Appendix D

Responsibility Matrix

Purpose: To identify all functions necessary to support an application running in the VDC and who performs each function.

Method of Completion: Existing templates can be used as a starting point, but each line item must be negotiated with all involved parties. The sample listed below conforms to the Modernization Partner model, however, for any given application, it may be necessary to add columns to accommodate additional participants.

Tips: Responsibility is indicated using the following codes:

P – Primary. This individual performs the function. Only one primary should be assigned to any activity.

A – Approval. It is assumed that some degree of concurrence is required for most activities. Use of the approval code should be reserved for cases where formal approval is required.

S – Support. Supporting groups will participate in the activity led by the Primary. There should always be a primary roles assigned to one participant in cases where supporting responsibility is indicated.

J – Joint. Joint should be reserved for activities where individuals will be performing their work relatively independently. For instance, each participant will be maintaining their own incident log. This is a joint activity.

See Appendix E

Due Diligence Checklist

Purpose: To precisely describe the maintenance activities to be performed by the VDC and to assure adequate preparation for receipt of the application by the VDC.

Method of Completion: The document should be reviewed with the VDC and concurrence reached. Back-up and archive requirements should be discussed with the business managers.

The document calls for information about the footprint and electrical requirements for the hardware. This information is only required if the hardware is being migrated to the VDC in addition to the software. If the VDC is purchasing and setting up the hardware, they will know this information.

Tips: The VDC does NOT have standard procedures that they follow for all applications.

You must specify exactly what the VDC must do to operate the system.

See Appendix F

Troubleshooting Document

Purpose: To support troubleshooting activities in an integrated environment by providing a description of all dependencies on other systems and among hardware items. This document is more critical for systems that are sharing resources with other applications, but should be done for all applications to depict all dependencies within the system.

Method of Completion: The document should be reviewed with the VDC and concurrence reached. Some of the hardware dependencies may need to be provided by the VDC and others may not be required since the VDC's Change Control Board performs configuration management. The application group should attempt to identify any expected occurrences and likely causes.

Tips: This is a living document. After each incident of unscheduled down-time some review of lessons learned should be conducted and this document should be updated as needed.

See Appendix G

Memorandum of Understanding

Purpose: To establish service level targets for up-time, and to define system availability.

Method of Completion: This document is negotiated between the business area, application support team and the VDC. Service levels are dependent on the level of hardware, software redundancy and the soundness of the processes surrounding the environment..

Tips: This is a living document. After each incident of unscheduled down-time a Root Cause Analysis will be conducted and the results will be communicated to the Business area, SFA CIO and the application support team.

See Appendix H

Run Book

Purpose: Internal VDC procedures for day to day maintenance the application

Method of Completion: The VDC will complete this document for review by the application team.

Tips: Applications member should review the document for completeness, and to assure that reports provided by the VDC will be adequate feedback.

See Appendix I

Other Useful Documents

Port Identification Form

This form is required to open ports on the firewall. The ports are specific to the applications and software tools being implemented. The source and destination IP addresses must be specified for each of the ports and the ports required must be specific. It is also important to specify all protocols or “listening” activities (ftp, http, etc.) that must occur on the port, and whether they are one-directional or bi-directional. Any nonstandard port request (i.e. ftp, telnet, http, etc) must be accompanied by a purpose so security risks can be analyzed.

See Appendix J

Hardware and Software Planning Template

This template can be used to clearly depict software and hardware requirements for a particular application. The purpose of this document is to be able to provide the staff at the virtual data center or IT Services a list so they can plan ahead to be able support such a configuration. This is a living document and should be updated as new software and hardware are added by the project. It is also a good location to document and track any issues that may arise as the architecture and applications are coming together.

See Appendix K

Operations Readiness Checklist

The purpose of this checklist is to ensure that all aspects of application design and development have been reviewed, key information is communicated, the documentation is complete, accurate and current, and agreements exist between the client groups, Applications Management and Operations Team and other support organizations where necessary. This checklist should be expanded to cover topics related to the specific technical design and appropriate tools as necessary. The *How Validated* section should be utilized to record validation information. If applicable items do not adequately meet the acceptance criteria, an issue should be identified and logged.

See Appendix L

The checklist is organized into the following sections based on project lifecycle:

- Client
- General
- Service Operations
- Service Recovery/Contingency
- Configuration Management
- Technical Architecture
- Code Review
- Security
- Testing

- Transition

Change Request Form

The purpose of this form is to provide VDC personnel and IT Services with all needed information for any requested change that will occur within the data center. This form is required to be completed for any change that will be made to an application that is currently in production. The project team must work with VDC personnel to ensure completion of all areas and submitted two weeks prior to scheduled change date. The change request must be reviewed by CSC and IT Services before the change can be approved and executed.

See Appendix M

New Services Work Order Form

The purpose of this form is to request any services from VDC personnel that is not included in traditional support provided by them. This form should be completed and submitted to IT Services for approval. The description of the task and budget information should be included in this form. Completion of this form is not required if the requested support is part of data center operational activities. Any questions should be directed to IT Services.

See Appendix N

Overview of Access Security Clearance, SFA IT Systems

Policy: *Access to SFA IT systems is granted only after appropriate investigation. This policy applies to employees both ED and its contractors.*

Roles and Responsibilities:

SFA is responsible for security on all SFA IT systems and facilities

Office of Inspector General's Security Staff maintains all security forms and performs investigations

SFA Security tracks which employees and contractors have completed security clearance

SFA IT Project Managers are responsible for granting access to their systems if and only if all other security requirements have been met.

Virtual Data Center Contractors are responsible for creating user names on servers upon receipt of signed Department of Education SFA Security Request Forms

ED LAN Contractors are responsible for creating user names on servers upon receipt of signed Account Request Forms

Applications Contractors are responsible for creating user names and allocating access within applications upon receipt of signed Department of Education SFA Security Request Forms

Personnel:

System Contact -- the person responsible for implementing these procedures for each individual system. This person submits security documentation to the SFA Security Personnel Representative for new access requests. This person may also assign user names and passwords if the individual system, and not the Virtual Data Center (VDC), controls user names and passwords.

VDC system access contact -- the person responsible for establishing user names and assigning passwords at the Virtual Data Center (VDC), when access is not handled by the individual system.

Neither the System Contact nor the VDC contact will assign user names for individuals who have not completed the clearance process.

SFA Personnel Security Representative -- the person responsible for overall SFA clearance operations. This person acts as the interface between SFA systems and the Office of the Inspector General's Security staff.

Procedures:

1. The access process starts with an authorized system manager, who identifies the level of access to be granted to the individual seeking access.

Security Levels:

- Minimal-risk,
- Non-sensitive (low risk),
- Medium-sensitive (moderate risk), and
- Highly sensitive (high risk).

Minimal-risk access involves read-only, or basic system functions that are protected by software edits. Example: data entry. By definition, Federal employees cannot be granted minimal-risk clearance.

Low-risk and Moderate-risk access involves more substantial access to system data and/or software commands, but such access is either reviewed by staff with higher-risk clearance, or protected by internal software edits and cross-checks, or both. Example: programmers.

The difference between low- and moderate-risk access depends on the vulnerabilities posed by the degree of access in question, and may differ from one system to another.

High-risk access involves the most substantial access to data and/or software commands, with less cross-checking or oversight by other staff. Example: system administrators.

The procedure for granting access continues when the system contact provides the applicant with an access form for the particular system. In addition to the system access request form, two forms are required of every applicant:

OF 306 -- Declaration for Federal Employment

Despite its title, all applicants, both Federal employees and contractor staff, must use this form.

Notice of Criminal Liability under the Privacy Act

Commonly called the "Privacy Act Form," this form describes the penalties available for misuse of Privacy Act information, and acts as notification of those penalties to applicants.

Other forms required are determined by the level of access to be granted:

Minimal-risk clearance requires only the OF 306 and Privacy Act Form as described above.

Low-risk (also known as the "1C") clearance requires the SF-85 (Questionnaire for Non-Sensitive Positions) and either the SF-87 (for Federal employees) or FD-258 (for non-Federal employees) fingerprint card. This level of request triggers a National Agency Check and Inquiry (NACI).

Moderate-risk ("5C") clearance requires the SF-85P (Questionnaire for Public Trust Positions), a Fair Credit Reporting Act Release, and SF-87 or FD258 as applicable. This clearance triggers a Minimum Background Investigation (MBI) or Limited Background Investigation (LBI).

High-risk ("6C") clearance requires the SF-85P, SF-85P-S (Supplemental Questionnaire for Selected Positions), a Fair Credit Reporting Act Release, and the SF-87 or FD-258. This request triggers a (full) Background Investigation (BI).

Employees with existing clearances granted through another agency (government or private) should provide a cover memo or letter indicating which agency granted the clearance, the level of clearance granted, and any other pertinent information. This will allow the ED Office of the Inspector General to retrieve information from the granting agency that maintained the clearance. This could take a week or two, and interim access cannot be granted during this time, unless it is for low-risk access where the security requirement can be waived. Usually, once the IG retrieves the data, SFA will accept the clearance, with no need to submit further paperwork, as long as the clearance level is appropriate and the staff has not had more than a year's break in service from the agency or company where the clearance was granted.

3. The system manager then submits all completed forms to the SFA Personnel Security Representative, who in turn submits applicable forms to the ED OIG Security Office.

The SFA Security Representative is Joel Clark, ROB-3 Room 4004, phone: 202-260-3739.

4. Waivers:

Employees with an existing clearance granted through another agency can submit information concerning that clearance (see Forms section above).

Contractor employees seeking read-only access, or low-risk access for less than 120 days, are considered *minimal-risk* employees and are granted access upon completion of the two basic forms (OF 306 and Privacy Act Form). All paperwork must be in the hands of the SFA Personnel Security Representative before such a waiver is granted.

Contractor employees seeking low-risk access for longer than 120 days must also complete the SF-85 and FD-258 fingerprint card, as described above.

Employees seeking moderate-risk (5C) access may be granted provisionary access to SFA systems provided that all paperwork has been submitted to the SFA Personnel Security Representative. In other words, access may be granted as the investigation is progressing, at the discretion of the System Contact and the SFA Personnel Security Representative.

Summary of Forms Needed by Risk for Contractor Employees

BACKGROUND INVESTIGATION FORMS NEEDED FOR NON-FEDERAL APPLICANTS FOR ADP SYSTEMS ACCESS

RISK LEVEL	CODE	SECURITY FORM	OTHER FORMS NEEDED	SUBMITTED TO OPM BY:
LOW RISK or NONSENSITIVE	1C	SF 85 "Questionnaire for Nonsensitive Positions"	FD-258 - Fingerprint Card OF 306 - "Declaration For Federal Employment" Notice of Criminal Liability Under the Privacy Act If employee has prior clearance, Cover Memo ADP system access form for each system Fair Credit Reporting Act Release MAY be required in some cases	Security Program Office
MODERATE RISK	5C	SF 85P "Questionnaire for Public Trust Positions"	FD 258 - Fingerprint Card OF 306 - "Declaration For Federal Employment" Notice of Criminal Liability Under the Privacy Act If employee has prior clearance, Cover Memo ADP system access form for each system Fair Credit Reporting Act Release	Security Program Office
HIGH RISK	6C	SF 85P "Questionnaire for Public Trust Positions" SF 85P-S "Supplemental Questionnaire For Selected Positions"	FD 258 - Fingerprint Card OF 306 - "Declaration For Federal Employment" Notice of Criminal Liability Under the Privacy Act If employee has prior clearance, Cover Memo ADP system access form for each system Fair Credit Reporting Act Release	Security Program Office

Summary of Form Descriptions and Usage

Form Number	Form Name	Description	Minimal Risk (Read Only)	Low Risk (1C)	Software Developer (5C)	DBA SA & CM (6C)
OF 306	Declaration for Federal Employment	Required for all applicants, both Federal Employees and Contractor staff	✓	✓	✓	✓
	Notice of Criminal Liability Under the Privacy Act	Required for all access	✓	✓	✓	✓
	EDNet Account Request Form	Required to get a user ID on the Education Network. EDNet access is not necessarily required in order to access applications at the VDC.	✓	✓	✓	✓
	Federal Pell Grant Rules of Behavior	Employees with EDNet Access who are working on Government Furnished Equipment (GFE)	✓	✓	✓	✓
FD-258	Fingerprint Card	Required for all access except Minimal Risk (Read Only)		✓	✓	✓
	Fair Credit Reporting Act Release	Required for all access except Minimal Risk (Read Only)		✓	✓	✓
	A Summary of Your Rights Under the Fair Credit Reporting Act	To be provided to all employees who complete a Fair Credit Report Act Release. Does not need to be submitted				
	Cover Memo Regarding Prior Clearance	Will expedite clearance in cases where clearance has already been granted elsewhere		✓	✓	✓
	Department of ED/SFA Security Request Form	One form is required for each system employee needs access to. Must be signed by the Education Project Manager for that System.	✓	✓	✓	✓
SF-85	Questionnaire for Non-Sensitive Positions	Required for Low Risk (1C) access. Available from www.opm.gov under Forms. Adobe .pdf files or special Forms Fill-in software that can be downloaded for free		✓		

Form Number	Form Name	Description	Minimal Risk (Read Only)	Low Risk (1C)	Software Developer (5C)	DBA SA & CM (6C)
SF-85P	Questionnaire for Public Trust Positions	Required for high risk (5C and 6C) access. Available from www.opm.gov under Forms. Adobe .pdf files or special Forms Fill-in software that can be downloaded for free			✓	✓
SF 85P*	Authorization for Release of Medical Information	Required for medium and high risk (5C and 6C) access. Last page on SF 85P. Available from www.opm.gov under Forms. Adobe .pdf files or special Forms Fill-in software that can be downloaded for free			✓	✓
SF 85P-S	Supplemental Questionnaire for Selected Positions	Required for high risk (6C) access. Available from www.opm.gov under Forms. Adobe .pdf files or special Forms Fill-in software that can be downloaded for free				✓

Procedure to obtain EDLAN network access

Fill out an Account Request Form (ARF) electronically and submit electronically to C.O.T.R.
See Appendix P for sample.

C.O.T.R. Submits electronic form(s) to Tawanda Hampton (Suite 6200, Portals Building)

This form is used to create an EDLAN user ID with the lowest (OC/Minimal-Risk) level of access, Basic office functions/software, e-mail, etc. Access to higher “security-levels” is based upon the forms and procedures detailed in section 4.

This form may be filled out by a contractor Task Leader but must be submitted to Tawanda Hampton by the C.O.T.R.

Note... An account request may be processed and an account assigned, but no software will be loaded on user/client systems until the new equipment has been properly checked into ED/SFA hardware inventory and an inventory barcode sticker has been issued and attached to the equipment. Once approved, user must call (202) 708-HELP to get technical support to install the SFA standard load.

Tawanda_Hampton@ed.gov

Questions/Hand-Delivery

**Tawanda Hampton
Portals Building**

Suite 6200

1250 Maryland Ave. SW.

Washington, DC.

202.401.2475 (voice)

202.260.5501 (fax)

Procedure to obtain EDNet Clearances

The Department of Education IT Security Office has identified 4 levels of access privileges;

- 0C - Minimal Risk, Read-Only
- 1C - Low Risk, Non-Sensitive
- 5C - Moderate Risk
- 6C - High Risk

Classification

As a general rule, IT users/employees are placed into the above categories based on function and need to access private data or otherwise sensitive material.

0C - Minimal Risk, Read-Only

Public Access, Ability to access their personal data/status indicators. no ability to change their data or access another customers data.

1C - Low Risk, Non-Sensitive

Basic (beginning) system user, access to non-sensitive job related data only. Ability to update job specific non-sensitive data only

5C - Moderate Risk

System software & business process developers, Quality Assurance & I.V.& V. analysts. Complete access to all sensitive and non-sensitive data as needed, restricted to off line or “non-production” systems. Read-Only access to “Production” system process definitions, source code etc. as needed. All “Write-Access” to the production systems routed through Quality Assurance and Configuration Management procedures.

6C - High Risk

System Administrators, Database Administrators, Configuration Management. Access to both Off-Line and Production systems. Authority to determine content and compliment, and validity of system components. Ability to reboot, backup, restore, recreate systems in whole or in part.

Clearances

The need for a specific clearance level is determined by the Task Leaders, Project Managers, C.O.T.R.s etc. Qualifying for these access privileges begins with the completion of a series of forms.

Employee Security Tracking Sheet

EDNet/VDC Security & Access Forms for:						
Item	Form Number	Form Name	Required	Date Completed	Date Submitted	Date Approved
1	OF 306	Declaration for Federal Employment				
2		Notice of Criminal Liability Under the Privacy Act				
3		EdNet Account Request Form				
4		Federal Pell Grant Rules of Behavior				
5	FD 258	Fingerprint Card				
6		Fair Credit Reporting Act Release				
7		A Summary of Your Rights Under the Fair Credit Reporting Act				
8		Cover Memo Regarding Prior Clearance				
9	SF 85	Questionnaire for Non-Sensitive Positions				
10	SF 85P	Questionnaire for Public Trust Positions				
11	SF 85P*	Authorization for Release of Medical Information				
12	SF 85P-S	Supplemental Questionnaire for Selected Positions				
13		Department of ED/SFA Security Request Form for _____				
14						

See Appendix O for Samples of Security Forms

This is a list of documents required for gaining access to SFA systems:

- OF 306 - Declaration for Federal Employment**
- **FD 258 - Fingerprint Card (Obtain form from Joel Clark. Instructions provided with form)**

-Fingerprint Options:

-ROB-3

- Room 5620
- Contact Doris Hold (202-708-6096) or
- Matt Baum (202-205-0785) to arrange a time.

-FBI Building

- 935 Pennsylvania Avenue
- 10am - 2pm, M-F
- Enter from 10th Street
- Inform guards that you want fingerprints taken
- 202-324-5853

-Arlington County Sheriff's Office

- 1425 N. Courthouse Road Suite 9100
- 1:30pm - 4:00pm, M-F
- \$10 charge
- 703-228-4252

-SF 85P - Questionnaire for Public Trust Positions (Available from www.opm.gov under Forms)

-SF 85P* - Authorization for Release of Medical Information (Available from www.opm.gov under Forms, last page of SF 85P)

-SF 85P-S - Supplemental Questionnaire for Selected Positions (Available from www.opm.gov under Forms)

-Security Request Form

-Notice of Criminal Liability under the Privacy Act

-Fair Credit Reporting Act of 1970 Release

- Federal Pell Grant Rules of Behavior

Procedure to Obtain VDC Access and Access to Other Applications

All security forms must be completed and access approved before a Contractor Employee can apply for access to a specific VDC server or application.

For access to all SFA applications, complete the Department of Education Student Financial Assistance (SFA) Security Request form. One form is required for each system.

Under section **C. Type of Access Requested**, specifics about servers, etc., must be completed. Servers must be listed by name or IP address to be clear to VDC personnel. Groups and access privileges should be included if known.

Under section **E. Signatures**, please note that the COTR/Security Officer and/or ED Project Manager refers to the Education employee responsible for that specific application.