

AIS Production Web Application Standards

Version 1.2

06/15/02

Table of Contents

Glossary	3
Introduction	6
AIS Infrastructure	
Goals.....	6
Definition of Standards.....	
6	
General Standards.....	
..6	
Security Standards.....	
.6	
Technical Standards.....	
7	
Operational Standards.....	7
Appendix A – Steps for Web Application Turnover and Management	9
Appendix B – Preliminary Web Application Questionnaire	10
Appendix C – Web Application Turnover Checklist and Signoff	11
Appendix D – AIS Infrastructure Checklist	13
Appendix E – Problem Management Procedures.....	15

Appendix F – Change Management	
Procedures.....	16
Appendix G – Management	
Issues.....	18
2	

Glossary

Acceptance Testing – This testing is done in an environment that closely simulates the production environment in order for the application to be “accepted” for production.

ASR – This is the Access and Security Representative for your work unit. The ASR enforces University policies and guidelines pertinent to the use of University computerized data assets. He/She acts as an interface between a specific work unit and the AIS Security Office.

Architectural Design – The blueprint that will ensure seamless integration with our existing application development infrastructure. A satisfactory integration methodology will comprise *all* of the following:

- Outline resource requirements.
- Identify the expected target population.
- Estimate the frequency of access.
- Select the appropriate hardware and software components.
- Define data access requirements.
- Ensure appropriate level of security integration.
- Comply with standard middleware interfaces, where appropriate.
- Describe any special programming techniques, where applicable.

Authentication – The process of verifying via User ID and password that a user is who they are supposed to be.

Authorization – The process of verifying via User ID and password that a user has been granted permission (is authorized) to access the system, function or data being requested.

Data Steward – A person authorized on behalf of the owner of the data to grant access to the data.

DCE – DCE represents the Distributed Computing Environment software, developed by a consortium of software vendors previously known as the Open Software Foundation (currently, the original consortium has all but disbanded and is also known as The Open Group). DCE consists of multiple integrated components including a Remote Procedure Call (RPC), Cell and Global Directory Services (CDS and GDS), a Security Service, a Distributed Time Service (DTS), Distributed File Services (DFS) and Threads. The RPC, CDS (or GDS), Security and Threads components are commonly referred to as the "secure core" and are the required components of any DCE installation. The Security Service provides a reliable way of determining if a user of a distributed system is allowed to perform a certain action, for example. DFS is an optional component. In addition, administration tools are available to help manage the various components.

DCE is also known as "middleware" or as an "enabling technology". It is not intended to exist alone and is usually bundled into a vendor's operating system offering or integrated via a third-party vendor. For example, DCE's Security Service component and Distributed File System can completely replace their current, non-network analogs. DCE

is not an application in and of itself but is used to build custom applications or to support purchased applications.

3

Digital Certificate – An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identifying information. The CA makes its own public key readily available through print publicity or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. The most widely used standard for digital certificates is X.509.

Enterprise Server – This is usually a class of server machines that provides primary access to **most** of an enterprise's electronic data. Platforms can vary but usually consist of a set of very large processors, large amounts of memory and adequate disk storage to hold large stores of data. One distinguishing feature of an "Enterprise Server"--as opposed to any other type of server--would be whether that server contains the **only** repository for the application data. By this definition, one could essentially define a smaller sized set of server machines as an "Enterprise Server". Today however, most people are referring to the mainframe environment when mentioning "Enterprise Server".

First Level Support – Personnel who provide front-line phone and email support for applications and services. This organization takes calls, records the information in a problem log and either solves the problem if it is possible at first level, or escalates problems depending upon severity to individuals within and outside of AIS.

Hot Spare Server – A spare server that is kept on hand, ready for duty in case of a hardware failure on a production server.

Installation Media – The disks, CD-ROM or other media that are shipped with a product or application for installation.

JAVA Applet – JAVA is an object-oriented programming language developed by Sun Microsystems. It allows executable programs called "applets" to be distributed over the World Wide Web. An applet is a small program, written in Java that travels from the Web server to the requesting client where it then executes. The applet part of the code, which is system-independent, is compiled and the result is called "bytecode". When a user clicks on a link that points to this bytecode, the bytecode is downloaded onto the user's machine. If the user is using an appropriate Java-aware Web browser, the browser contains an interpreter (specific to the user's machine) which interprets the bytecode and allows the user to run the applet.

JAVABeans – Reusable Java classes that can be manipulated and customized in Java program development environments. These classes can be linked together to create applets, applications or even new beans for reuse by others.

4

Penn State DCE Cell – Presently, Penn State supports **one** large "DCE cell" that consists of a DCE Security Service--aka the Security Registry--and a Cell Directory

Service (CDS). There is also a replica cell maintained for backup and/or fail-over protection. Users of services are defined in the cell as principals. Services provided via the cell are also defined as principals. These services may be software and/or hardware components. Within the cell, principals are defined in pre-established "Groups" that are used to establish access control criteria. Access control is managed using "Access Control Lists" (ACLs). This is the part of DCE that manages authorization of service. The "Penn State DCE Cell" is managed and maintained by the Center for Academic Computing (CAC).

Software Licenses – The physical licensing agreement for software ownership.

System Documentation (when writing, include reference to:)

- Web application structure and flow diagram (indicate all external calls).
- List of all calls to other resources and a brief description of their function. (e.g.: calls to various resources on the Enterprise Servers including databases and port numbers, eCommerce calls, external database accesses, etc.)
- List of all files that will need to be put on the server. (Examples include: programs, DLLs, configuration files and Java files) Also indicate which files to include in scheduled backups.
- List of any known Frequently Asked Questions (FAQ).
- Indicate what security is required for users to access the system. If access is restricted to a group or groups, who is allowed and how is membership determined?
- List of personnel who will need access to test servers.
- Error recovery instructions if normal procedure of restarting the application is not adequate.

5

Introduction

The purpose of this document is to define the standards for production web applications that are managed by AIS. Any web application proposal, which does not adequately comply with prescribed doctrine, may be rejected.

AIS Infrastructure Goals

Our goals in managing all production web applications and servers are to:

- Maintain the security and integrity of the data associated with the application.
- Provide a high performance and reliable service to the application's users.
- Provide 100% availability during the advertised hours of operation of the application.
- Provide sufficient monitoring capabilities of the application and server to permit rapid detection and recovery should a failure of the application or server take place.
- Automate the application and server environment to the point that human intervention is only required for:
 - (a) Integrating upgrades/fixes to the production application or server;
 - (b) Recovery from application, server, or data failures.

Definition of Standards

General Standard:

1. Follow steps identified in Appendix A. Each new or updated web application requires completed checklists. (See Appendix B, C and D).

2. Since it is impossible for any single person to judge the operational impact that application changes may have on the rest of the organization, it will be necessary to complete, at a minimum, Steps 1-3 in Appendix A for all application changes that are adding functionality (changes that are correcting errors or introducing clarifying text to an application are excluded from the process).
3. For each application, there will be one (primary) person and one (backup) person who is responsible for coordinating application issues with Infrastructure.

Security Standards:

1. All user authentication and authorization for restricted access is accomplished by confirming User ID and password combinations in conjunction with pre-established DCE group definitions in the Penn State DCE cell.
2. System access requests are approved and processed by the user's Access and Security Representative (ASR).
3. All data has a designated Data Steward that approves any access request outside of a predefined access paradigm.
4. Digital certificates from an accredited certificate authority are used on all secure Web Servers.
- 6
5. All servers will use Secure Socket Layer (SSL) transmission encryption.
6. Automated logging of all successful and unsuccessful access attempts is performed.
7. Physical access to server hardware is restricted to authorized individuals.

Technical Standards:

1. Architectural design (including DCE integration analysis, data access technique, and component selection) is a joint decision of the development staff and AIS Infrastructure.
2. Each application is continuously monitored by software that provides automated alerts when the application is not functioning properly. The current preferred method is the VisualWave Application Monitoring Tool (Future consideration will be given to providing an automated event-notification system from within the application itself).
3. Automated server and application activity logs are generated.
4. An automated reporting mechanism is used for all activity logs.
5. Installation media and software licenses for all server software are centrally managed.
6. At least one installation media copy and software license for each piece of client software is centrally managed.
7. Acceptance testing is required prior to production implementation.
8. All production web source code and system documentation is maintained in a centrally-located repository.
9. Single-purpose server environments are maintained only where justified (i.e. any given production server will only perform functions associated with a single application).
10. Automated procedures are used to update data on intermediate and back-end servers.

Operational Standards:

1. Problem resolution follows the prescribed Problem Management Procedures (See Appendix E).
2. First level support is provided weekdays between the hours of 7:30 a.m. and 5:00 p.m.

3. All client-based software is distributed using an approved automated procedure.

4. A web site for application system documentation is provided and maintained.

5. A single Hot Spare Server is available for emergency use only.

6. System and application software and data files are backed up weekly.

Supplemental

backup and recovery procedures are provided on an application-by-application basis.

7

7. All changes to the production environment follow the prescribed Change Management Procedures (see Appendix F).

8

Version 1.1

Appendix A - Steps for AIS Web Application Turnover and Management

If you are developing or making major revisions to, a Web application that will be managed by Administrative Information Services, you must follow the steps identified below. The completion of this process will ensure the successful turnover and ongoing management of your application.

Step 1 – Review the **AIS Production Web Application Standards** document.

Step 2 – Submit a **Preliminary Web Application Questionnaire**.

Currently, all web application forms need to be printed, completed and submitted to Carl Seybold in paper form. Future versions of the forms will be interactive.

Step 3 – Attend **Preliminary Web Application Meeting**.

Prior to starting application development, contact Carl Seybold to schedule your first meeting with AIS Infrastructure personnel.

In this meeting, you will discuss the architectural design, the technical requirements of your application, timeframes for your work and review potential issues in Appendix G. A tentative production target date will be established in Step 4.

Step 4 – Attend **Web Application Planning Meeting**.

Once application development has begun and you have an idea of how long the programming may take, contact Carl Seybold to schedule your second meeting with AIS Infrastructure personnel. This meeting will be to discuss any new requirements and establish a tentative production target date. This meeting must take place at least 90 days before final production. Following this meeting, Infrastructure will start the AIS Infrastructure Checklist in Appendix D.

Step 5 – Complete the **Web Application Turnover Checklist** prior to Production planning meeting.

Step 6 – Attend **Web Application Production Planning Meeting**.

Contact Carl Seybold to schedule your production planning meeting with AIS Infrastructure personnel. This meeting must take place at least 30 days prior to tentative target production date.

In this meeting, you will review the Web Application Turnover Checklist, demonstrate the final application to Infrastructure personnel and discuss application support and management issues. Infrastructure will in turn describe where they are in

completing the AIS Infrastructure Checklist. If no problems are identified in this meeting, a final production target date will be established.

Step 7 – Receive sign-off from AIS Infrastructure, AIS Support and Consulting and Support Services.

In order to confirm that all steps have been completed to move this application into production, these Directors and managers must sign off on the Web Application Turnover Checklist.

9

Version 1.3

Appendix B - Preliminary Web Application/Server Questionnaire

Application Name _____ Date _____

1. Provide a brief description of the purpose of this application or server **and attach a general flow diagram:**

2. Please identify the following:

Primary contact: Name _____ Phone _____ Email _____

Server and operating system requirements _____

Intended audience for the application including estimate of peak number of concurrent users _____

Will the application need a digital certificate? Yes _____ No _____

Should this application be monitored with AIS' current monitoring software? Yes _____ No _____

Will the application use DCE authentication? Yes _____ No _____

If not, please indicate why: _____

3. Will the application retrieve Enterprise Server data? Yes _____ No _____

Will the application update Enterprise Server data? Yes _____ No _____

If yes to either, please describe the mechanisms for retrieval/delivery of data.

4. Will the application require access to data or applications on servers other than the Enterprise Server data?

Yes _____ No _____ If yes, please specify.

5. Will your application use Java or Active X to perform functions? Yes _____ No _____

6. Will Cookies need to be permitted by the browser? Yes _____ No _____

7. What are the planned hours of availability for this application?

8. Will the development environment be different from Smalltalk and VisualWave? Yes _____ No _____

If yes, please describe the software being used.

9. Is there a new command (glue or action routine) being implemented on the Enterprise Server (mainframe) to support this application? Yes _____ No _____

If so, please list: _____

10. Please indicate any target dates that have been discussed:

10

Version 1.2

Appendix C - Web Application Turnover Checklist

Application Name _____ Date _____

Application Developer Tasks - Development

1. The following documentation should be attached to this checklist:

- Web application structure and flow diagram (indicate all external calls).
- List of all calls to other resources and a brief description of their function. (e.g.: calls to various resources on the Enterprise servers including databases and port numbers, eCommerce calls, external database accesses, etc.)
- List of all files that will need to be put on the server. (Examples include: programs, DLLs, configuration files and Java files) Also indicate which files to include in scheduled backups.
- List of any known Frequently Asked Questions (FAQ).

2. What security is required for users to accessing the system?

If access is restricted to a group or groups, who is allowed and how is membership determined?

Application Developer Tasks – Acceptance Testing (2-4 weeks before target date)

1. Has the application been through acceptance testing? Yes ____ No ____

2. Are all application-specific files contained within a single directory (or sub dirs)? Yes ____ No ____

3. Are all HTML, image, or other Web resources in their appropriate directories? Yes ____ No ____

4. If there are any application-specific web/e-mail reports, did they function correctly? Yes ____
No ____

5. If there are any Enterprise Server calls, did they function correctly in test? Yes ____ No ____

6. Does the application access any databases outside of the Enterprise Server? Yes ____ No ____

Were the ODBC connections set up correctly? Yes ____ No ____

Did the database accesses work correctly? Yes ____ No ____

7. Does the application use activity logs? Yes ____ No ____

If so, were they tested in acceptance? Yes ____ No ____

Give the filenames (and directories) of the log files:

How are the logs viewed /retrieved? Are archives necessary?

8. Has an application-specific monitoring capability been successfully interfaced with
Infrastructure monitoring tools? Yes ____ No ____

9. Will this application have on-line documentation such as FAQs associated with it? Yes ____
No ____

10. Does this application have a specific time frame of heavy activity? Yes ____ No ____

If so, please indicate average number of users and the time frame:

Application Developer Tasks – Production & Deployment

11

1. What is the minimum browser version needed to use the application?

PC MAC

Netscape Navigator: _____

Internet Explorer: _____

Other: _____

The application requires: Cookies Javascript ActiveX Java



2. If the application requires special actions when restarting, please explain those:

3. Primary contact for the application:

Their preferred method of contact (email address or phone number):

Please indicate the name and phone number of the contact during the first 24/48 hours of production implementation if it is different than the primary contact:

4. Please specify the name and electronic mail id of the primary contact for maintaining on-line documentation such as FAQs?

Web Application Turnover Sign off

Signatures for all individuals below must be present in order for your application to be moved in to production. This is used in Step 7 of the turnover process.

Mike Belinc

Director, Infrastructure
Administrative Information Services

Clyde LeFevre

Director, AIS Support
Administrative Information Services

John Williams

Manager, Access & Accounts
ITS - Consulting and Support Services


12

Version 1.2

Appendix D - AIS Infrastructure Checklist

Application Name _____ **Date** _____

Infrastructure Tasks

 1. Order or identify existing hardware and software necessary for the application testing, acceptance and production. This will include:

Server hardware (shared/new)

Server operating system

Application server software

- Digital certificate Yes ____ No ____
- Other security software as needed (i.e. Security Adapter)

- Integration with monitoring software











- Network port to backbone

- IP address / DNS entry

- AD/DS Account




- Environmental requirements (space, electrical, etc.).

- Cybex console/keyboard control ports/cables


-  2. Implement an administrative account and unique password for the server. Document this administrative account and password in the server security list and store in safe area.
-  3. Implement server hardware, operating system software, application server software, web server, digital certificate and other security software.
-  4. Centrally manage installation media and software licenses for all server software and at least one media copy and software license for client software.
-  5. Connect server(s) to the network.
-  6. Implement monitoring software.
-  7. Establish weekly automated TSM backup of application server unless specified differently by the developer.
-  8. Establish mechanism for application developer to request updates to production server.
-  9. Integrate server with Cybex console controls.
-  10. Provide information on the following to the Application Developer: server hardware and software, TSM backup schedule, monitoring information, location for all code and system documentation, port numbers, IP address/host name, mechanism for integrating production changes and schedule for applying production changes.
-  11. Provide information to AIS Support staff detailing the following:
 - Enterprise Server requirements
 - Any special operational procedures needed for the application.

13

Infrastructure Tasks - Continued

-  12. Maintain a single Hot Spare server for emergency use.
-  13. Provide monitoring information including contact list and guidelines to AIS Support and Consulting and Support Services staff for use during and outside of, normal business hours.
-  14. Sign off on production turnover of web application.

Consulting and Support Services Tasks

-  1. Ensure that Consulting and Support Services personnel are trained to provide first level support for all applications during normal business hours. This includes taking calls, recording problems and escalating those that cannot be solved on first level.

- ✎ 2. Monitor all applications supported by AIS during normal business hours.
- ✎ 3. Augment application FAQs and answers, as specific issues are uncovered.
- ✎ 4. Sign off on production turnover of web application.

AIS Support Tasks

- ✎ 1. Ensure that operators are trained to monitor identified applications outside of normal business hours and escalate problems identified as “critical” to third level contacts provided by the Application Developer.
- ✎ 2. Provide any database support needed for the web application.
- ✎ 3. Sign off on production turnover of web application.

14

Appendix E - Problem Management Procedures

Consulting and Support Services is the front-line contact with customers. This support is provided during normal business hours, Monday through Friday. The problems are logged in a database, solved whenever possible and escalated if that is not the case.

Consulting and Support Services must have a record of the third level contact for each application. This ensures that appropriate personnel are notified if the application appears to have a problem that is not caused by the unavailability of an external resource.

Once a developer has been notified of an application problem, it is their responsibility to keep Consulting and Support Services informed of the resolution. Consulting and Support Services requires this information to close the problem and keep the users informed.

Emergency Backup/Restore

At any time during the implementation process, the developer may deem it necessary to restore the Backup image to production. If this occurs, Infrastructure personnel should be notified to initiate this.

15

Appendix F - Change Management Procedures (Currently under Review for Updates)

What is change management?

Change management is the procedure defined for facilitating and controlling updates to the production environment. Every attempt will be made to automate this process so that it is streamlined yet provides the control essential to maintaining a stable production environment.

How does it work?

The automated procedure for moving non-emergency updates of VisualWave applications into production occurs nightly. The timing of this process is justified for several reasons. Most importantly, it is critical that usage in a production environment not be disrupted during the day for updates. Therefore, implementations of new or updated applications occur only during non-production hours, unless an Operation Critical situation is identified.

The standard process will involve the use of DFS (Distributed File Systems) storage space for placement of files. This technology allows us to utilize DCE (Distributed Computing Environment) for secured access. The standard procedure will be to have group space defined on DFS for VisualWave applications. For each application, there will be one person (primary) and a backup who is responsible for coordinating the update of images for that particular application with Infrastructure. These two contacts will be given access to the DFS directory defined for the application and will place images and

other files in the appropriate subdirectories when an update is desired. It will be the responsibility of the development coordinator (or their backup) to ensure that all of the appropriate files get transferred to Infrastructure via DFS.

DFS will be used for both acceptance testing and final production turnover. The difference is that for production, a nightly procedure will move images out of designated areas into production. For acceptance testing, the application developer will move their own images into the acceptance area for testing. In the production environment, the new image will go into effect with the nightly restart of the server(s).

Developers will be given the ability to restart the image on the acceptance server. They will be responsible for determining whether or not to change an image during the day. By giving the developer the capability to move images into acceptance themselves, we have enhanced the process a bit to provide more freedom to the developers. However, along with freedom, comes responsibility. It is the developer's responsibility to minimize the impact to others when changes are moved in to the acceptance environment.

An example of how the DFS directories will be set up is:

```
\\...\dce.psu.edu\fs\depts\oas\servers\newserver
```

subdirectories

```
... \newserver\backup  
... \newserver\production  
... \newserver\new  
... \newserver\log  
... \newserver\acceptance
```

16

Example: The automated procedure runs each night and checks the NEW subdirectory. If the files there have later dates than those in production, the images will be moved from the NEW subdirectory into the PRODUCTION subdirectory. Before this happens, the procedure will move the existing production image into the BACKUP subdirectory. If major problems occur, the image in the BACKUP subdirectory will be brought back into production. It is the developers responsibility to notify Infrastructure if they see a problem with the application that requires the BACKUP image to be restored.

How do I get access to DFS?

If you are not an AIS employee, information about obtaining the DFS client and support can be found on the web page: <https://www.work.psu.edu/access/dce/> . If you are an AIS employee and don't already use DFS, you should contact Consulting and Support Services to obtain the necessary site-licensed software. In either case, once you have installed the DFS client, send an email message to AIS-servers@email.AIS.psu.edu to request DFS space for your application.

What exactly is the process?

Once you have access to the appropriate DFS directories for your application, use the following procedure to initiate a non-emergency update of a VisualWave Application.

For Production Images

1. The developer will have Read/Write/Delete/Update access to the appropriate DFS NEW subdirectory. Image files should be copied into the appropriate DFS NEW subdirectory during production hours and they will automatically be moved that night. The developer does not need to request this move since the process is automated. An automated electronic mail notification will alert identified personnel of the update. The

image(s) will be live once the services have been restarted in the morning. **This process does not yet exist.** In the meantime, send an e-mail message to AIS-servers@email.AIS.psu.edu to request the update to a production image.

For Acceptance Images

1. For acceptance testing, the application developer will be granted Read/Write/Delete/Update access to the appropriate DFS ACCEPTANCE subdirectory. The developer will use this subdirectory to store a new image for acceptance testing. The developer will be provided with a mechanism to restart the service for their application.
2. Acceptance testing will be standard and moving images from testing to production will always involve the acceptance testing step.

17

Appendix G - Management Issues

1. Hardware

- a. What department will purchase the needed hardware?

- b. What department will provide funding for upgrades?

2. Software

- a. What department will purchase the needed software?
- b. What department will provide funding for upgrades?
- c. To whom will the software be registered?
- d. Who installs the software? (operating system, specialized applications)
- e. Who provides support for the specialized software?
- f. Who purchases the digital certificate if a unique one is required?
- g. Who will generate informational web pages about this application including FAQs?

3. Physical Plant

- a. What department will purchase any additional Physical Plant requirements as a result of new applications?

- b. What department will fund expanded Physical Plant requirements?

4. Telecommunications and Networking Services Items

- a. What department will purchase any additional telecommunications equipment required as a result of new applications and servers?

5. Personnel Training

- a. Who will provide funding for training AIS staff to use new hardware, software, etc.?

- b. Who will provide funding for increased staffing requirements?

- c. What department is responsible for funding backup costs?