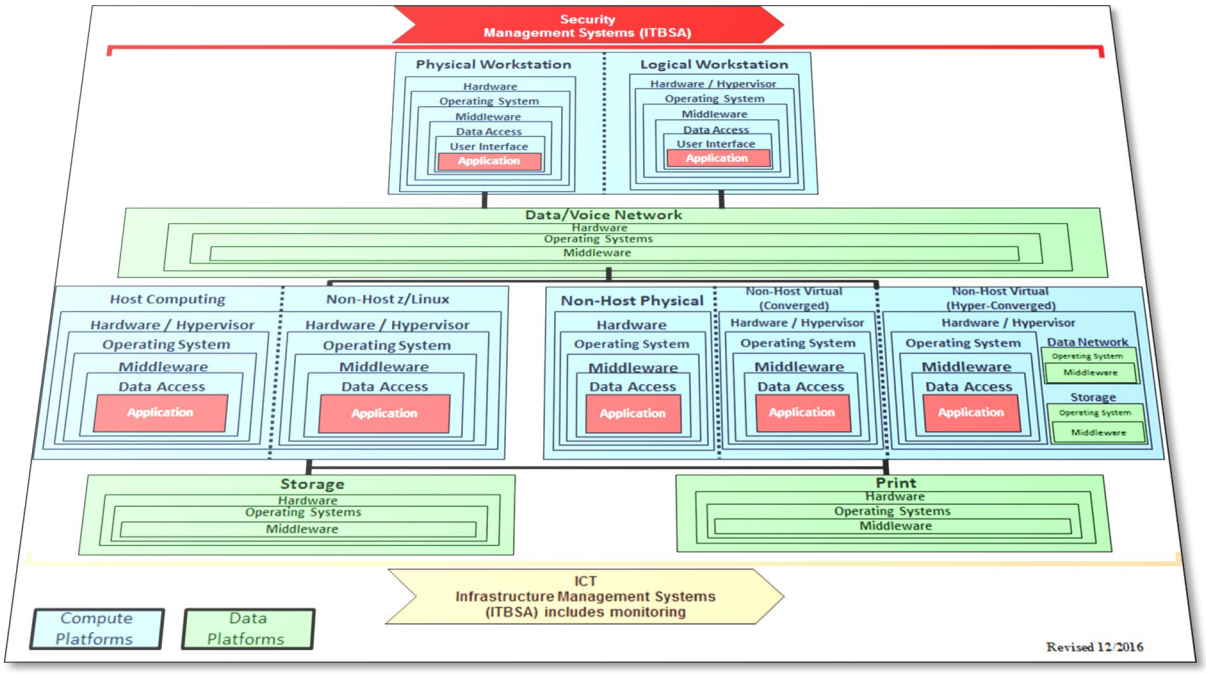
South Carolina

BlueCross BlueShield of South Carolina is an independent licensee of the Blue Cross and Blue Shield Association

imagination to Implementation i2 INFORMATION TECHNOLOGY

Technical Standards — Infrastructure



Information Systems Standards Manual

Table of Contents

Table of Figures

There are currently no figures in this volume.

List of Tables

Chapter 1 Overall Technical Infrastructure Standards

IN THIS CHAPTER

This chapter contains standards that are applicable across the board for BlueCross BlueShield of South Carolina Information Systems.

1.1 System Documentation

System Documentation is created with the initial introduction of a system, which is any application and/or infrastructure or group of such that comprises a complete or partial business solution. System Documentation is maintained during the life of the system and must be updated as a part of any subsequent or relevant Work Request.

Appropriate System Documentation meets the following objectives, which should guide determination of what information is considered relevant:

- Repository for practical institutional knowledge
- Reflection of the current state of the system
- A work reference for developers to make modifications, fix errors, or implement requirements
- A guide to the system for other roles
- Awareness for project teams during the project life cycle
- An introduction for new team members

The requirements for System Documentation outlined in this chapter are designed to produce documentation that meets these objectives and is informative for all roles. While System Documentation must, at a minimum, meet these requirements, the System Documentation for certain systems may exceed them.

However, not all requirements will be applicable to all systems. Personnel creating and updating System Documentation must be familiar enough with the system or work with the Technology Owner listed in System Master Index (SMI) to determine which requirements are applicable to the system in question.

System Documentation may be created and maintained in whatever format is most appropriate for the system if it meets the requirements outlined in this chapter. The storage location of system documentation must also be specified in SMI.

Any application or infrastructure that is a component of a single larger system may be addressed through the parent System Documentation. If the application/infrastructure comprises its own system or is part of multiple systems, it must have its own documentation.

1.1.1 System Documentation Components

The sections that follow provide requirements for the components that make up the System Documentation.

1.1.1.1 References to Existing System Documentation

To avoid duplication of information, wherever applicable, refer to existing System Documentation to meet the System Documentation requirements outlined in this chapter. All referenced System Documentation must meet the update and review requirements outlined in the section *System Documentation Updates and Reviews* below.

1.1.1.2 Security Compliance

To affirm compliance with relevant security requirements, System Documentation must include the following statement:

> *This application/system follows all applicable guidelines listed in the BlueCross BlueShield of South Carolina Corporate Policies and the Information Systems Standards Manual (ISSM). This includes, but is not limited to, access control, security assessment and authorization, configuration management, contingency planning, and system and services acquisition.*

System Documentation should indicate any other applicable security controls for all business areas supported by the system. This must include a listing of exceptions to the applicable controls by risk document number.

NOTE System Documentation should not be shared with non-I/S Work Request participants. If a non-I/S Work Request participant requests a review of this documentation, Client Management should request approval from the Application Manager

1.1.1.3 Abstract

An abstract approximately 250 to 300 words in length must be included first as an at-a-glance description of the system. This will be used by Architects, Designers, and other roles who will need to quickly understand the purpose and qualities of a system.

1.1.1.4 System Overview

A System Overview is a narrative description that provides a reader with a clear and concise description of what a given system does and includes, the business functions it satisfies, and includes the features and business functions it supports, and should be approximately one page in length.

The System Overview will also identify the primary internal and external customer areas that use or depend on the system as well as any other directly dependent business areas. It must also identify the SMI number for the system.

1.1.1.5 Glossary

All system-specific terms or abbreviations or both must be defined and explained within the System Documentation.

1.1.1.6 Diagrams

System Concept Diagrams

Relevant system Concept Diagrams must be included or referenced in the System Documentation. The I/S Enterprise Architects site in Microsoft SharePoint includes a repository for Concept Diagrams approved by the Enterprise Architects.

Non-Host Bridge Diagram

For non-host systems, if a full, current bridge diagram exists it must be included as part of the System Documentation. Bridge diagrams should be stored within the SharePoint documentation site for the latest Work Request. Contact I/S Engineering for further assistance obtaining bridge diagrams.

Presentation Application Storyboard and Business Logic

References detailing the business logic of the system must be provided as part of the System Documentation.

If Presentation Application Storyboards for the system exist, they must also be supplied.

User Interface

If the system has a user interface (UI), provide diagrams and descriptions of the UI for all functionality described in the System Documentation.

System Flows

Create a high-level diagram showing the sequential flow of functional steps. It is not necessary to identify every detailed step.

Flow Diagrams

The System Documentation must also include any other pertinent flow charts that will help to support the system, such as job flow diagrams and MQ flow diagrams.

Develop a call chart for any program that calls other programs and include it in the System Documentation. The chart must provide a pictorial view of the system, the calling programs, and the called modules.

Non-Host Application System Flows

The System Documentation for a web-based Presentation Application will also include the following:

- Site Map — A high-level diagram showing navigation structure. The map should include a summary of the site navigation, global functions, constituents, content and all other pertinent information to the browser-based, front-end design.
- Functional Web Page Flow — A flow chart showing process and web page flow.

1.1.1.7 System Interfaces

Create a high-level interface chart to show how the various components interrelate with each other. Include interfaces with other systems, subsystems or vendor packages.

List the Host systems and the method used to interface with that system (e.g., CICS transaction, MQSeries, AFP2Web, SMTP, FTP, cloud).

When applicable, each interface method will have a table by function outlining the specific transaction or method used by the application when interfacing with other systems, infrastructure or applications. Provide a high-level description for each item. The table could include:

- Customer
- Function
- Transaction ID
- Map name
- Transaction description
- Web service name

1.1.1.8 Business Impact

Document the system's impact on the business, including dependencies that will be impacted in the event of an interruption. The System Documentation must also address any applicable service level agreements.

1.1.1.9 Roles, Responsibility & Access

List the roles required for the development and operation of the application as well as summarizing the responsibilities and secure access requirements for each.

Refer to *Security Management* for more information on system security.

1.1.1.10 Workstation Requirements

Specify all workstation requirements for any role that may work with the system. Indicate if there are specific forms or approvals for requesting needed drivers, applications, etc.

1.1.1.11 Infrastructure

Provide a listing of all infrastructure that supports the system or application. This includes production and lower environments and all relevant platforms (host, non-host, network, etc.). Details about technical requirements, configuration, and purge criteria must also be included where applicable.

Production infrastructure is also required to be listed in the Disaster Recovery plan. It is acceptable to refer to the Disaster Recovery Plan where applicable as it must also be linked within the System Documentation. However, non-production infrastructure must still be listed.

1.1.1.12 Technical Overview

System Code Components

Provide high level descriptions of all relevant host code modules or non-host Application Program Interfaces (APIs) that are called from the system and their known dependents.

System Technical Components

Address requirements for all applicable items below:

- Software repositories
- Application system accounts
- Firewall rules
- Network location
- Host components
    - Driver and sub-driver programs
    - Special compile or build considerations (such as Package Binds, subschema, token names) for this system
- Non-Host components
    - Programming language and version
    - Toolkits or other add-ons
    - Data connection types and version
    - Minimum and recommended workstation configuration for both developers and end users, including Citrix storefront availability and package names
    - Application-specific, minimum server requirements, include clustering and virtualization
    - Application/tool dependencies, listings of open-source and vendor-owned software and versions
    - Storage
    - Application system accounts
    - Databases
    - Ports, protocols, and services (PPS)
    - Drivers
    - MQ
    - MFT
    - VRU
    - Telephony
    - Web services

Data Files

List all relevant non-temporary data files that are used within the system. For example:

- File name and descriptions
- Database tables
- Type of data source (DB2, IMS, VSAM, etc.)
- Network shares
- Access (Read, Write, Update)
- Data owner

Data Dictionary

If applicable, identify the location of the Data Dictionary for each of the data files listed in the subsection *Data Files* above. When necessary, refer to manuals where dictionary definitions or descriptions reside.

System Outputs

List all relevant system outputs such as reports, correspondence (e.g., letters, EOBs, checks, etc.), transmission files, mail-out tapes and other electronic media.

- Description
- Program name that creates the output
- Report numbers
- Any other relevant system outputs
- Host-based outputs

    - INFOPAC identifiers
    - Content Manager On Demand (CMOD) document types (where applicable)
    - Type of transmission (e.g.,Connect:Direct, FTP, etc.) for files transmitted to other data facilities

Non-Host System Outputs

List all relevant system outputs where the Presentation application is the source of data collection used to create the output. Output can be in hard-copy form or data that is passed to another system using a 3270 interface, MQ or ODBC, or cloud solution. Examples could include INFOrm records, claim records, enrollment forms or correspondence.

This list must include, where applicable:

- Description
- Program name or page that creates the output
- Report numbers
- Form or identifying factor
- Any other relevant system outputs

Source Configuration Management

Provide a description of the Software Configuration Management (SCM) tool that directs I/S Staff to the source code when needed.

For Non-Host applications, document the Code Staging Process including the following:

- List the tools used to manage different versions of configuration objects created during software development.
- List the tools used to manage and preserve versions of all identified documents in the development process.
- List all staging software and servers with enough detail to be clearly identified. Mention any special move considerations.
- Describe or diagram the process that transmits all deliverables to a production release.
- Include any relevant information for package and infrastructure readiness.

The SCM database for the system and the location of the system within the SCM database must be identified in SMI.

1.1.1.13 Vendor Information

Vendor-owned applications require separate System Documentation if the application comprises its own system or is utilized by multiple other systems. Requirements for vendor applications utilized by a single system must be addressed as part of the system technical components of the parent system.

If there are components or configuration of a vendor-owned application that are managed by the organization, System Documentation should define what is managed by the organization as opposed to the vendor.

System Documentation for vendor-owned applications is required to meet the same requirements outlined in this chapter. There may be components that are expressly not applicable for certain vendor-owned systems.

Where applicable, provide links to vendor documentation to meet the System Documentation requirements outlined in this chapter. At a minimum, the documentation must provide links to the following vendor documents:

- Installation and setup documentation
- User interface references
- System flows
- Administrator documentation
- User guide

If the above vendor documents are not available, then the absence must be noted and explained.

1.1.1.14 Testing

Describe the testing environment for all platforms. Describe the procedures required to ensure successful implementation including helpful hints and special considerations. This information must include an overview of the following:

- Unit Test procedures
- System Test procedures
- Load Testing procedures
- Qual Test procedures
- Production verification procedures

1.1.1.15 Monitoring

List the system or application monitoring used, including infrastructure and security monitoring, along with a summary of the process for tracking and responding to monitor alerts. Include a brief description of what activity or resources are monitored.

1.1.1.16 Procedures

Post Implementation Procedures

State the follow-up actions needed to ensure successful implementation. Include specific system output and procedures that must be verified.

Security Access

Indicate the security system used to access the system or its components. For example, indicate if security is controlled at the RACF, Active Directory, DB2 table or file level. Provide the process for a user to be able to request security access, for administration, maintenance, or testing, including internal users of external facing websites/apps.

For those applications that have integrated security systems, the documentation needs to include sufficient level of detail to cover the following topics:

- Instructions on verifying and processing system access/maintenance requests
- Application security sign-on procedures
- Process for new hire and terminated/transferred requests
- Requirements for administrator access
- Process for timely reviews of users and access capabilities
- Description of security-related reports, run frequency, contents and distribution
- Differentiation of authentication and authorization control

Refer to *Security Management* for more information on system security.

Operational, Maintenance, and Troubleshooting Support

Provide details and/or procedures for operational support, system maintenance, and troubleshooting. At a minimum, provide the following:

- Configuration procedures
- Link to incident management procedures
- Support points-of-contact
- Troubleshooting guidance
- Relevant Technology Support Center self-service forms
- List of application service accounts

Disaster Recovery

Each system must have its recovery procedures addressed in a Disaster Recovery Plan (DRP), and the DRP number must be entered into SMI. You can access the plans in SharePoint Online.

Requirements for Disaster Recovery Plans are detailed in *Service Management > Service Delivery > IT Service Continuity Management > Disaster Recovery Plans*.

The following System Documentation requirements are also required in whole or part by the current Disaster Recovery Plan requirements. It is acceptable for System Documentation to refer to the Disaster Recovery Plan, where applicable, if the plan is linked within the SDM:

- System Interfaces
    - Downstream dependents and processes

  - Upstream dependencies

- Data Files
  - Data Requirements

- System Technical Components
  - Workstation Requirements
  - Firewall Rules

- Vendor documentation

1.1.1.17 Scheduling/Processing Times

Detail the schedule for processes and jobs performed by the system. Include the relevant platforms and interfacing systems for each process/job.

1.1.1.18 Licensing

If applicable, System Documentation must include a current account of client access licenses (CALs) including assessment of CALs needed and counts of available and utilized CALs. Explain how the organization meters and assigns CALs for the system. Include related processes for requesting, recycling, and other general management of CALs.

1.1.1.19 Prospection

Where applicable, describe the planned future state of the system including, but not limited to:

- Unused features that may be utilized in the future
- Architectural direction and strategy
- System roadmaps

1.1.1.20 Additional Relevant Information

Any additional relevant information that is applicable to meeting the stated objectives of System Documentation must be captured, such as key performance indicators (KPIs), threat models, or additional subject matter experts or points-of-contact.

1.1.2 System Documentation Control Requirements

1.1.2.1 System Documentation Updates and Reviews

Updating the System Documentation is a required task for any significant Work Request following the System Development Methodology.

In this context, "significant" are those, by Work Request or otherwise, that add, remove, or meaningfully modify a business function or architectural structure. If other system interfaces, diagrams, and flowcharts are updated, the new versions should be incorporated into System Documentation.

Additionally, System Documentation must be reviewed at least every three years. Reviews as part of a system update fulfills this requirement. If no system updates occur in a three-year timeframe, a full review of the System Documentation must be performed and recorded within the document history to ensure all details are up to date.

After completing updates to System Documentation, changes must be approved by the Technology Owner identified in SMI and documented in the document history.

1.1.2.2 Document and Work Request History

Significant Work Requests or System Documentation reviews and updates should be recorded in the document history. Each entry must contain the following:

- Update trigger (Work Request number or periodic review)
- Implementation date or date of document change
- Identity, role, and I/S area of the person updating the System Documentation
- Description of system update (if applicable)
- Summary of document changes
- Identity of Technology Owner and date approved

1.1.3 System Documentation Manual

A System Documentation Manual (SDM) must be made available to provide I/S staff with a high-level overview of the interfaces with other systems, inputs, outputs and documentation on systems that require I/S support. The SDM furnishes a high-level overview, reflects the current state of the system, and creates a knowledge base to quickly identify "Start work" points to make a modification, fix an error, or to accommodate a new requirement.

Chapter 2 Hardware

IN THIS CHAPTER

This chapter contains standards that are applicable to the computing and networking hardware used at BlueCross BlueShield of South Carolina.

2.1 Host Hardware Naming Conventions

All Host hardware in the data centers fall in the following categories with the appropriate naming conventions. Typically, hardware is identified by the vendor model name; however, there are two levels of naming conventions within the Host environment that identify particular equipment. These names are determined by the zO/S System Programmer and identify the subsystem name and operating system address. A list of examples of the hierarchy of naming standards for the Host hardware categories is listed below (Table 2-1). Category descriptions follow.

Examples of the Hierarchy of Naming Standards for Host Hardware Categories

Category	Actual Model	Subsystem Name	System Address Name
CPU	2964-724	2964C	SYSA, SYSD, SYSJ, SYSK
Virtual Tape	3957-V07	TLIB003A	1D00-1DFF
Physical Tape	3592-E07	TLIB001A	1100-1129
Physical Tape	3592-E07	None (Stand Alone)	1F0
Direct Access Storage Device (DASD)	DS8886	None	9000-9FFF
Printer	IP4100	PRT4	PRT4

Table 2-1 Examples of the Hierarchy of Naming Standards for Host Hardware Categories

2.1.1 CPU

From a Host hardware perspective, the current model number that is installed on the floor identifies each Mainframe. Since model numbers change throughout the life of a particular footprint installed, the zO/S System Programmer identifies Mainframe CPUs by the base CPU model type followed by an alpha character based off the order the Mainframe was installed. For example, for subsystem name 2964C, 2964-724 is the actual model installed. In this example, 2964 would be the base IBM model number, and C would be the third CPU installed.

2.1.2 Virtual Tape

From a Host hardware perspective, the actual equipment model identifies each Virtual Tape Subsystem (VTS). The zO/S System Programmer identifies the subsystem name by **TLIB00XY**, where **X** is the number that the subsystem was installed into the Host environment, and **Y** is an alpha character that describes any peripheral components associated with the VTS. For example, 3957-V07 is the actual equipment model. Subsystem names equal TLIB001A, TLIB003A, and TLIB003C. TLIB001A would be the first VTS installed in the Host environment where TLIB003A would be the third. TLIB003C identifies another component of TLIB003A. Once the subsystem name is determined, a system address

range is given to the subsystem. No basis exists for what the actual system address names are. The names are chosen from an address range that has ample sequential hexadecimal values to satisfy the total quantity of drives that the device is capable of having installed.

These system addresses must be unique in the SYSPLEX environment, meaning that there cannot be two devices with the same system address name.

2.1.3 Physical Tape

From a Host hardware perspective, their actual equipment model type (e.g., 3592-E07) identifies physical tape drives. If the physical tape drives are housed within an automated tape robot, the zO/S System Programmer will identify the physical tape drives within a subsystem name (e.g., TLIB001A). The number and alpha character following **TLIB00** is determined by the next available combination that has not been defined within the Mainframe environment. Within this subsystem name, the physical tape drives are given operating system address names (e.g., 1100-1129). No basis exists for what the actual system address names are. The names are chosen from a system address range that is consistent with similar devices installed. These system addresses must be unique in the SYSPLEX environment, meaning that there cannot be two devices with the same system address name. If a physical tape drive is not installed within an automated tape robot, no subsystem name will be given, and the device will just have a system address name known to the operating system.

2.1.4 Direct Access Storage Devices

From a Host hardware perspective, Direct Access Storage Devices (DASD) are identified by the actual equipment model type (e.g., DS8886). The zO/S System Programmer identifies each subsystem with its unique address range known to the operating system. No basis exists for what the actual system address names are. The names are chosen from an address range that has ample sequential hexadecimal values to satisfy the total quantity of drives that the device is capable of having installed. These addresses must be unique, meaning that there cannot be two devices with the same address name.

2.1.5 Host Printers

From a Host hardware perspective, Host Print subsystems are identified by the actual equipment model type (e.g., IP4100). The zO/S System Programmer identifies each subsystem with its unique address range known to the operating system. No basis exists for what the actual system address names are. The names are chosen from an address range that has ample sequential hexadecimal values to satisfy the total quantity of drives that the device is capable of having installed. These system addresses must be unique in the SYSPLEX environment, meaning that there cannot be two devices with the same system address name.

2.2 Infrastructure Software Configuration Management

System Modification Program Extended (SMPE) is a software configuration management tool that we use to install and apply maintenance to most z/OS vendor software (e.g., z/OS, CICS, DB2, etc.). Some vendors utilize other tools. We use the CA ENDEVOR software configuration management tool and follow ENDEVOR procedures to apply changes or customizations to internally-developed software.

2.3 Data Network Standards

2.3.1 Data Network Infrastructure Index

2.3.1.1 Local Area Network (LAN)/Wide Area Network (WAN) Infrastructure

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is an IP standard designed to reduce the complexity of administering address configurations by using a server computer to centrally manage IP addresses and other related configuration details used on the network. The workstation sends a *BOOTP* request, which is forwarded to specific DHCP servers throughout the network. The DHCP server will supply the workstation with a TCP/IP address, domain name (bcbssc.com), and enough information to allow basic network communications. The TCP/IP address is *leased* to the workstation for a short period of time. Typically the address lease is *renewed* automatically by the workstation, but allows flexibility when workstations move from one location to another, to lease a new address that is valid for that geographic location without any manual configuration required.

Domain Name System (DNS)

Domain Name System (DNS) is the name resolution protocol for TCP/IP networks, such as the Internet. A DNS server hosts the information that enables client computers to resolve memorable, alphanumeric DNS names to the IP addresses that computers use to communicate with each other. It's much easier to remember names than addresses. For example:

The DNS server would translate mye-work.bcbssc.com to the TCP/IP address 10.80.17.54. For names outside of our domain, the server would forward the query to external DNS servers to translate www.scstatehouse.net <http://www.scstatehouse.net> to 167.7.215.69.

LAN Wiring Standards

BlueCross BlueShield of South Carolina follows Local Area Network (LAN) wiring standards set by the Institute of Electrical Engineers (IEEE), Electronic Industry Alliance/Telecommunications Industry Association (EIA/TIA) and the National Electric Code (NEC). These organizations are alliances of manufacturers, educational institutions, and government agencies that have come together for the purpose of setting industry standards for the manufacturing and installation of telecommunications components. The primary standards that apply to us are:

- IEEE 802.3 — Access methods and physical layer specifications for Ethernet
- IEEE 802.5 — Access methods and physical layer specifications for Token Ring
- IEEE 802.8 — Specifications for Fiber Optics
- IEEE 802.11 — Specifications for Wireless LANs
- EIA/TIA 232 — LAN Physical Layers
- EIA/TIA 568B — Commercial Building Wiring Standards
- NEC — Rules for the installation of Telecommunications cabling (as adopted and enforced by local law)

We also require that component manufacturers be ISO 9001 certified.

The type (or category) of Unshielded Twisted Pair (UTP) copper cabling that we run to the desktop is mandated by EIA/TIA 568B:

- CAT-3 is rated for voice or 4/16MB Token Ring
- CAT-5e is rated for 10/100MB Ethernet
- CAT-6 is rated for 10/100/1000MB Ethernet

2.3.1.2 Core Network

Channel Interface Processors (CIPS)

We use CISCO Channel Interface Processors (CIPS) equipped Routers to connect our network to our IBM Enterprise Servers.

We utilize both CISCO 7507 Routers (with Cisco Systems Network Architecture (CSNA)) and CISCO 720X Routers (with Channel Port Adapters (CPA)) to provide mainframe connectivity to our Systems Network Architecture (SNA) nodes. While the CIPS/CPA support both the ESCON (fiber) Channel Adapter (ECA) and the Parallel (Bus and Tag) Channel Adapter (PCA) cabling standards, we only implement ESCON type connections in our network.

Core Switches

Network Services defines a Core Switch as being a Systems Enterprise Class Switch being used to support the network Backbone. Our current standard is the CISCO Nexus 7000 series with a Supervisor 2 Engine. The Switches must provide nothing less than 440 Gigabits per second switching capacity on the Back Plane. They must also support redundant Supervisor Engines, redundant Power Supplies, and a modular architecture for ease of upgrade.

2.4 Voice Network Standards

2.4.1 International Voice Communication

2.4.1.1 Establishing International Voice Communication Internal Voice

International access will be established only when a completed **Phones - Moves/Adds/Changes** Service Request has been authorized by an Assistant Vice President (AVP) or above.

2.4.1.2 Removing International Voice Communication Internal Voice

Communications will be removed only when a completed **Phones - Moves/Adds/Changes** Service Request has been authorized by an AVP or above.

2.4.2 Silent Monitoring

2.4.2.1 Establishing Silent Monitoring

Silent Monitoring will be established only when a supervisor or manager completes an **Authorization to Silent Monitor Calls** Service Request, which is located on TSC Self-Service. The form requires the supervisor's or manager's phone number and a list of the automatic call distributor (ACD) groups to be monitored. Prior to submitting the security form to Telecom using the email address VOICE.TELE, the supervisor or manager must obtain a Vice President (VP)-level approval.

Once the form has been received by the assigned Voice Platform Operations technician, they will then make the appropriate configuration change to add the **Service Observe** feature to the requestor's phone. A copy of the form will be stored by the technician in the ICT NH Network & Telecommunications Deployment site in ***SPO***.

2.4.2.2 Removing Silent Monitoring

When a supervisor or manager leaves or moves to another area/role, the assigned Voice Platform Operations technician will remove the **Service Observe** feature from their phone using the Avaya phone configuration.

2.4.3 Voicemail Standards

A request for voicemail access is submitted using the **Phones - Moves/Adds/Changes** Service Request.

A default password is established at the time the user profile is created. The first time the mailbox is used, the user is prompted to enter a new password, from four (4) to 15 digits in length. Voicemail user profiles are not created for an extension that has not been assigned a unique name.

Voicemail setup instructions are located on My e-Work under Tools > Telephone System Information.

Chapter 3 Operating Systems

IN THIS CHAPTER

This chapter contains standards that are applicable to the operating systems used at BlueCross BlueShield of South Carolina.

3.1 Production Update Schedule

The purpose of this section is to provide a schedule for production updates by system. Any deviation from this schedule must have departmental management approval.

Any change to a production cycle that could/does affect any other production cycle, i.e., predecessor change, etc., must have permission, in writing, for such change from both areas' management. Signatures on the corresponding move sheet constitute such permission.

3.1.1 Schedules

3.1.1.1 Production Implementation Schedule for All Batch Systems

All batch system changes and PROC updates will be moved into production on THURSDAY.

3.1.2 CICS/APS Online Program Moves Responsibility Procedure

These procedures outline the action to be taken and the responsibility for the moving of new programs or changes to existing Customer Information Control System (CICS) and APS online programs.

3.1.2.1 Tasks Completed on Friday

- All production moves must be completed by 5:30 a.m. on Friday. In addition, using the Service Request process through the Technology Support Center Self-Service Portal, a Service Request must have been sent to the move coordinator listing the affected programs.
- Contact the online "MOVE" coordinator from Tactical Services and give him/her the name and phone number of the person who will be the I/S contact.
- The I/S contact person will be notified at approximately 6:30 a.m. on Friday morning that testing may begin. Notification will be via Phone mail.
- All programs and maps to be moved into production should be entered in the Endevor system prior to 5:30 a.m. on Friday. Any programs or maps to be moved that are not on the "MOVE LIST" by 5:30 a.m. will require approval of the Tactical Services manager.

3.1.2.2 Tasks Completed on Friday Morning

- Check the move list. Coordinator sees if there are any modules that start with OL00, MM04, MM05 or MM06. If there are, the AMMS background adjudication system will have to stop via the transaction. After the moves and the "New Copies," start online adjudication via the "OLDY" transaction. See the "OLDY" documentation for the use of this transaction.
- If any task has taken an excessive amount of transaction dumps or taken any storage violations, back it out.
- Verify with each I/S contact person that their changes either did or did not work. If there is any question, back it out.
- Notify Tech.Support when all testing is complete.
- On Friday morning following the moves, notify the manager of the Tactical Services Department of all modules that were backed out.

- On Friday morning following the moves, insure that the appropriate Software Developer has been notified of all modules that were backed out.
- After all testing is completed, Tech Support will move online programs from BC.NDVR.STAGE.CICSLIB to BC.NDVR.CICS.EXCPLIB. These moves are normally done on Fridays.
- After a program is moved into "EXCPLIB," it will be moved to "PRODLIB" by Tech Support on Wednesday of the following week. CICS Software Developers do not move programs in or out of "PRODLIB." Tech Support maintains “PRODLIB.”

3.1.3 Emergency/Special CICS Program Moves

Implementations of new or modified CICS programs outside of the scheduled Friday morning implementation schedule should follow the outline below (Table 3-1).

Emergency/Special CICS Program Moves

Responsibility	Action
Application Area	Create and cast Endevor Package containing CICS programs to be moved into Production. This package must begin with a ‘**#**’ Contact Technical Support to schedule move of the elements and the NEWCOPY. If the package contains a new or changed Online planbind, contact the DB2 On call DBA to schedule the bind. A DB-Help request must be submitted. Following the package execution, verify that all components are installed and active.

Table 3-1 Emergency/Special CICS Program Move

Use the ISPF Callout panel – U.10.15.4.1.4 to identify the NEWCOPY and BIND contacts.

U	Custom
10	Applications
15	Toolbox
4	Production Support
1	System Callout
4	Find Person on Call for Abending Job

Use **CICS** as the Jobname to identify the person who will perform the NEWCOPY.

Use **DB2DBA** as the Jobname to identify the person who will perform the BIND.

3.2 Production Acceptance

3.2.1 Production Acceptance — Turnover Procedures

The purpose of this section is to explain the procedure that will be used for the turnover of all production jobs. This procedure will pertain to modifications that affect the scheduling of existing production jobs as well as new jobs. All scheduling changes, including new jobs, must be accompanied by a Production Control Log (See the section *Production Control Log* below).

Test jobs (operating in ZEKET) will follow the same standards as production jobs with the exceptions described below.

3.2.1.1 Submission Procedures

A completed Production Control Log (PCL) for production; TESTPCL for Test and related materials (see below) must be submitted via the Service Request process to cause the production acceptance process to begin. The submission procedures are based on the type of changes being made to a given job.

NOTE If the submission procedures are not followed and changes are placed into production, the manager of the programming area responsible for the changes will be responsible for the balancing and distribution of reports until proper submission procedures are followed.

Submitting a "New" Job

All JCL, DOCULIBS, etc., must first be moved into production. The Production Control Log (PCL) and all related materials must be submitted to Scheduling five (5) working days prior to the scheduling of the first production execution of the job. If the change affects the current schedule, a separate PCL must be submitted to Scheduling indicating "Temporary Scheduling Change" each day until the request has been processed and the scheduling database has been updated. Where required, PCLs must be submitted to the appropriate Systems Support area to be forwarded to Scheduling.

All New Jobs must have a valid on-call reference in Toolbox prior to production acceptance.

Balance Procedures

If balancing procedures are involved, the "Programming Area" will schedule a walkthrough with the "Distribution Area" during this five (5)-day period to review the balancing procedures. The submitting Software Developer should arrange a time for this review when the Production Control Log is submitted. If the Distribution Area is already aware of the changes, they must be notified of the first live production date. Not required for Test jobs.

Changing Existing Jobs without Distribution Affects

If submitting changes to an "EXISTING" job and these changes do not affect distribution or balancing procedures but does affect scheduling constraints:

The DOCULIB must first be updated in production. The Production Control Log and all related material should be submitted to SCHEDULING three (3) working days prior to the scheduled production execution of the job. If the change affects the current schedule, a separate PCL must be submitted to SCHEDULING indicating "TEMPORARY SCHEDULING CHANGE" each day until the request has been processed and the scheduling database has been updated. Where required, PCLs must be submitted to the appropriate Systems Support area to be forwarded to Scheduling. Standards for DOCULIB members are described in the section *Production Acceptance — Job Documentation* below.

Changing Existing Jobs which Affect Distribution

If submitting changes to an "EXISTING" job and these changes do affect distribution procedures:

The Production Control Log and all related material must be submitted to SCHEDULING when the proc update containing the changes is submitted.

Changing Existing Jobs which Affect Balancing Procedures

If submitting changes to an "EXISTING" job and these changes do affect balancing procedures, refer to *Technical Standards — Applications > Application Coding > RULEs Standards and Guidelines > Balancing and Reconciliation Processing Requirements* for procedures and JCL for automated balancing.

The Production Control Log and all related material must be submitted to SCHEDULING three (3) days before the first scheduled production execution of the job.

The "PROGRAMMING AREA" will schedule a walkthrough with the "DISTRIBUTION AREA" during this three (3)-day period to review the balancing procedure. It is suggested that the submitting Software Developer arrange a time for this review when the Production Control Log is submitted.

3.2.1.2 Explanation of "Related Materials"

The following is a brief explanation of the various "RELATED MATERIALS," which may be required, depending on the situation.

If there is a parameter card that must be maintained by Scheduling: The name of the member on a given Software Developer's PDS, Staging jobdeck or in ENDEVOR, which contains the "EXECUTION JCL" (i.e., Job Card, Execute Card, and Parameter Pointer). Scheduling will copy this into the permanent JCL library. JCL updates are processed for NON-ENDEVOR areas only.

Most parameter cards will be stored in the PDS by the name "BC.SCHD.ZEKE.CNTL." Any parameter cards required for the Test system will be maintained by programming.

A separate member has to be set up for each card if in a different proc. These will be updated through TSO daily via the edit function. The execution JCL must include the dataset with the parameter card member name. Example for two cards in different steps for one job:

Example: Verify that a member does not already exist in CNTL PDS. card one for PCWJ20D is "PCWCC20D."

```
EX. SYSIN DD DSN=BC.SCHD.ZEKE.CNTL(PCWCC20D),DISP=SHR
CARD TWO FOR PCWCJ20D IS 'PCWCC20X'
EX:  SYSIN DD DSN=BC.SCHD.ZEKE.CNTL(PCWCC20X),DISP=SHR
```

All parameter cards should be automated if possible. Justification is required for all parameter cards via the Service Request process and should be submitted at the same time the Production Control Log is submitted for the documentation change. Refer to *Technical Standards — Applications > Application Coding > Date Considerations* for guidelines concerning the use of parameter cards. JCL updates must be submitted via the Service Request process.

The member name of the member on staging jobdeck, which contains the NON-ENDEVOR proc update for a given job. SCHEDULING will move this update into the production proclib.

All static control cards (i.e., Utility Statements) must have been placed on BC.NDVR.PROD1.CARDLIB or BC.NDVR.PROD1.VSAMLIB by the submitting Software Developer. If the card cannot be automated, written justification should be submitted to SCHEDULING.

If major changes are made to balancing procedures for "EXISTING" jobs or when submitting a "NEW" job, sample reports from a systems test must be submitted to DATA CONTROL and reviewed with the "OUTPUT SECTION" of DATA CONTROL as explained above. Refer to *Technical Standards — Applications > Application Coding > RULEs Standards and Guidelines > Balancing and Reconciliation Processing Requirements*.

3.2.1.3 Requests for Scheduling/Submission of On-Request Jobs

Once an on-request job is set up in the Scheduler, there are three ways to request execution.

1. Provide the Service Request process with the pertinent information.
2. Using the Service Request process, all 'U' job requests should contain the following information (Table 3-2):

'U' Job Requests

Requestor Information	Submitted By
Department	User Supplied
Job Name	User Supplied
Extension	User Supplied
Parameter Card Format Information	User Supplied

Table 3-2 'U' Job Requests

3. A PCL may be filled out with the pertinent information.

In all cases: All requests for U jobs to be run must be in SCHEDULING by 2:30 p.m. If received after 2:30 p.m., the job will not be scheduled until the next working day. Where required, these requests must be sent to the appropriate Systems Support area, which will forward them as needed depending on the time of day.

Rejection Procedures

If the above data is rejected for any reason by SCHEDULING, it will be returned to the originator based on the criteria outlined below. The reason for rejection will be indicated through the Service Request process.

If submitted 5 days prior to execution, it will be returned within 3 days after receipt.

If submitted 3 days prior to execution, it will be returned within 1 day after receipt.

3.2.1.4 Acceptance Procedures

When the above data is accepted for production, SCHEDULING will be responsible for the following:

Updating the job to the automated scheduling system database, according to run sequence specified in documenter.

Notifying OPERATIONS of the new job and any special considerations necessary while running.

NOTE Under ENDEVOR/MVS, Production Coordinator moves procs to BC.NDVR.PROD1.PROCLIB.

Distribution will be responsible for the following:

- Deciding on a due out time and coordinating this with the user department receiving the output.
- Creating or updating check off sheets using distribution specified in documenter.
- Writing balancing procedures using information obtained from documenter.

3.2.2 Production Acceptance — Job Documentation

The purpose of this section is to provide documentation for each production job. Job Documentation includes: Job Documentation Narrative and Job Analysis Documentation.

3.2.2.1 Job Documentation Narrative

Each production job must have a documentation member narrative stored in "BC.NDVR.PROD1.DOCULIB" for jobs under Endevor/MVS change control. The job narrative must contain the following information. (Format note: each line in the narrative must be coded as though it is a comment card in a JCL stream.)

I	Job narrative (Job name and short explanation of what job does.)
1.00	Simple description of what job does and PROC(s) used by the job
1.01	Scheduling Requirements: Indicate exactly how job is to be run. (e.g., Run Tuesday thru Sunday at 5:00 a.m.). "If Applicable" items are not "required". If left out, they will be disregarded by Scheduling.
	• Predecessor Job Names or Dataset Names. Must use "NONE" if there are no predecessors.
	• Operator OK if applicable: Use if job is to be loaded on "hold".
	• Specific day or date job is to be scheduled. (Daily indicates a Monday thru Friday run frequency.)
	• If job is run according to a customer or Software Developer supplied schedule, indicate this in 1.01.
	• Specific Job Start Time, if applicable. "Early AM" is unacceptable.
	• Calendar ID if other than default calendar of "A" or use of Special Calendar. Indicate Special Calendar name if applicable.
	• Group ID if applicable.
	• Application ID if applicable.
	• Saturday cycles have application IDs to allow for easier viewing and maintenance.
	• Late Time if applicable.
	• Event Suffix if applicable.
	• Some areas have jobs run with variable predecessors. The event suffix is used as a trigger.
	• Retain Event, YES or NO (Should event be retained at new schedule load?) RETAIN = YES – Event is to be retained at new schedule load. RETAIN = NO - Event is to be dropped at new schedule load.
1.01A	Disaster Recovery Scheduling Requirements If 1.01A indicates "yes," the job will be considered part of critical system recovery in the event of an actual disaster. A production disaster test is scheduled annually. All or most areas will be participating. We need the DOCULIB to indicate if the job is part of the disaster recovery cycle & if there are different preds, indicate it. Example: This job will run as part of disaster recovery for Memb with normal preds.
1.01B	Holiday Scheduling Requirements If your job is to be scheduled on the holiday; indicate it & any special instructions. Example: Job runs on a holiday as normal with CS99J99D as only pred. This section is completed if your job is run "ON" the holiday. Normal

	holiday scheduling will not change.
1.01C	Special Cycle Scheduling Requirements Several areas scheduled special cycles "Saturday" on a regular basis. If the job is to part of a special cycle, indicate this and any changes to the way the job is normally scheduled. Example: This job is part of any special Saturday cycle.
	If there are no specific requirements, write "NA" where applicable. Violation of these standards will result in the rejection of the job documentation
1.02	Complete balancing procedures including job and report numbers
1.03	Report description of all reports in this job and distribution
	• Report number:
	• Form number:
	• Description: User header information
	• Distribution: User department name
	• INFOPAC No.: Reference ONLINE or BATCH or Both
1.04	Description and layout of all records such as date cards and parameter cards. All parameter cards should be automated or placed on CARDLIB. (Refer to *Technical Standards — Applications > Application Coding > Date Considerations* for guidelines). If date cards or parameter cards are "NONE", 1.04A and 1.04B do not apply (effective 12/01/2000).
1.04A	Date and parameter cards updated by Scheduling
	DDname layout update frequency
1.04B	Other date and parameter cards
	DDname layout update frequency updated by
1.05	If the GTM file is used give the table header control transaction number
1.06	Is CICS affected by this job? Yes or no
1.07	"IS" Total used? List functions performed and backup and restore procedures
1.08	Is IMS/DB used? List functions performed and backup and restore procedures

	----------
II	Controlled Abend code (1 code per line).
2.01	Explanation of code and action to be taken.

III	System Abends (1 code per line).
3.01	Abends that are programmed

IV	Restart and rerun procedures.
4.01	At what point (job and step name) should the restart be attempted? What datasets should be deleted or overridden? What changes must be made to date cards parameter cards or control cards?
V	Other instructions.
5.01	Any additional operations or control information such as tapes to be mailed and addressed; any other special scheduling scenarios such as the use of SCOMs and ZEKE resource name and condition code scheduling information for use of ZEBB Restart/Rerun product. Resource information will be provided by Scheduling.

Resource Example

Resource Example

Resource Name	CNT	Codes	Step	Proc
		MD H E A	Name	Name
AUDTD	001	SR Y R N		

Table 3-3 Resource Example

Condition Code Example

Any condition code greater than zero should result in an ABEND.

Condition Code Example

Step Name	Proc Step	Operator	Range	Action
EOJ CC			Low High	
********	********	GT	0	A

Table 3-4 Condition Code Example

3.2.2.2 Job Analysis Documentation

Automated analysis of production jobs is also available via an automated documentation package. Refer to *Technical Standards — Applications > Application Coding > RULEs Standards and Guidelines > Balancing and Reconciliation Processing Requirements*.

3.3 Production Control Log

The purpose of this section is to provide an explanation of the Production Control Log and how it should be completed.

Test jobs (operating in ZEKET) will follow the same standards as production jobs with the exceptions described below.

The Production Control Log (PCL for production; "TESTPCL" for Test) is the communication vehicle through which the programming staff requests services from the Scheduling department via the Service Request process. The Service Request should be routed to Scheduling.

3.3.1 Production Control Log Contents Explanation

A Production Control Log will be submitted to Scheduling for any of the following reasons: Cutoff times are as follows:

- Temporary scheduling changes, Overrides - 2:30.
  Restarts - all RESTARTS and ABEND requests should be submitted using Batch Response Ticket in INFO, this includes any Test Jobs.

NOTE When submitting a PCL to affect changes on new or existing jobs, please submit one PCL per job change.

Production restarts after 5 p.m. are to be referred directly to Computer Operations.

Requests received after specified cutoffs will not be processed until the next working day unless a hardcopy PCL is submitted with area manager's signature.

3.3.1.1 New Job

When submitting a new job. Lead time required — 5 days (See the section *Production Acceptance* above.)

When submitting a request to setup a new job, please supply the date the job is to go into production if it is after the initial five day turnaround.

3.3.1.2 Change to Existing Job

When submitting updates to an existing job. Lead time required — 3 days (See the section *Production Acceptance* above.)

3.3.2 Temporary Scheduling Change

When submitting a request to make a change to the scheduling of any job in the current cycle. Do not use this block for normal documentation updates. It is to be used for changes to the current scheduling cycle only. A PCL may be used to request the scheduling of a "U" (user-request) production job. Other acceptable methods are described in the section *Production Acceptance* above.

3.3.2.1 Deletion of Jobs

When taking job out of production.

3.3.2.2 JCL Change

JCL change to the permanent library (i.e., job card or exec card). New job JCL is not updated until documentation is approved; must be submitted via area's System Support Account for Non-Endevor areas only. All others will be handled by programming through Endevor moves.

3.3.2.3 PROC Update

Under Endevor/MVS, PROC updates will be performed by the Department production coordinators and not Scheduling.

For areas not under Endevor/MVS, a Production Control Log for PROCLIB changes must be received by Scheduling by 11:30 a.m. on Thursday. PROCLIB update runs will be done at 11:30 a.m. and 2:00 p.m. The 2:00 p.m. run will be for corrections and special requests only. Special requests must be accompanied by written approval of the area director. Area code must be included in all Production Control Logs for routing purposes. Special runs needed other than Thursday are for emergencies only and are to be submitted no later than 11:30 a.m. on the day they are needed via the Service Request process. Scheduling will process PROC updates received daily, therefore, it will be the programming area's responsibility to insure only "Emergency" updates are submitted on Monday, Tuesday, Wednesday and Friday. Do not submit DOCULIB updates on same production control log as PROC updates.

3.3.2.4 DB2 Update

Does job access DB2. If yes, job will be scheduled after 5:00 p.m. Request will be rejected if field not completed.

3.3.2.5 Override

To be used when requesting an override to be used in Production JCL.

The override and appropriate parameter card should be placed into the affected JCL and the updated member should be saved in a staging job deck. Override requests should be in Scheduling by 2:30 p. m. on the effective date of the change. The override is used for the current cycle only.

3.4 Removal of Job from Production

The purpose of this section provides an explanation of the procedures to be followed when removing a job from a production cycle.

Test jobs (operating in ZEKET) will follow the same standards as production jobs with any exceptions being described below.

3.4.1 Removal of Production Job Permanently

3.4.1.1 Job is Under Endevor Control

1. To remove a job from production or test that is under Endevor control, the appropriate JOBDECK(T) and DOCULIB(T) elements must both be transferred to ARCHIVE.

    a. The Endevor TRANSFER to ARCHIVE must be done at least five working days prior to the effective date of the change.

NOTE The DOCULIB element must be archived first. It can be archived in an earlier package, or in the same package but listed first. Endevor will not archive a JOBDECK element unless the DOCULIB element has already been archived. As with all packages involving production jobs, Systems Support will be required to give final approval and execute the archive package

---

    b. No PCL is required to notify Scheduling to remove the job. Once the transfer to archive is successful, the name of the job is written to a special PDS to notify Scheduling that it is to be removed from production.

2. If the archived job affects the current schedule, a Service Request must be sent to Scheduling via the Service Request process indicating that this job is being archived and should no longer be scheduled to run. Also state the job name and stop run date.

    a. Cutoff for receipt of the email by Scheduling is 3:30 p.m.

3. Scheduling will complete the following actions:

    a. Monitor the special PDS for new modules.

    b. Scheduling will remove the job from the ZEKE scheduling database.

    c. The execution JCL will be removed from the ZEKE JCL PDS.

    d. The parameter card(s) will be removed from the CNTL PDS.

    e. Scheduling will not be sending a "notification of completion" email to the Software Developer. Scheduling will have completed the removal process when the JCL can no longer be found in BC.SCHD.ZEKE.JCLLIB.

3.4.1.2 Job Is Not Under Endevor Control

1. A Production Control Log (PCL) must be completed by the programming staff and submitted to Scheduling. Where required, this must be sent first to the appropriate Systems Support area, which will forward it to Scheduling.
2. The PCL will indicate the job name(s) to be removed from production and the reasons for the removal. For both Production and Test jobs, use the Service Request process.
3. The PCL must be received at least three working days prior to the effective date of the change. If the change affects the current schedule, a separate PCL must be submitted indicating "TEMPORARY SCHEDULING CHANGE" each day until the request has been processed and the scheduling database has been updated. Cutoff for receipt is 3:30 p.m.
4. Scheduling will complete the following actions:

    a. Deactivate event upon receipt of PCL as long as current schedule has loaded.
    b. Verify the DOCULIB member has been deleted or archived by Software Developer before job can be taken out of production.
    c. Scheduling will remove the job from the scheduling database.
    d. The execution JCL will be removed from the permanent JCL PDS.
    e. The parameter card(s) will be removed from the CNTL PDS.

NOTE Removal of a job temporarily requires a Service Request submitted to Scheduling via the Service Request process requesting jobs be "deactivated." As with PCLs and Run Sheets, where required this Service Request must be sent first to the appropriate Systems Support area, who will forward it to Scheduling.

3.4.2 Standards for Using the Test Scheduler (ZEKET)

This section documents the standards for placing test jobs and test cycles into the Test Scheduling System (ZEKET). These standards apply to new jobs as well as to modifications that affect the running of existing test jobs within ZEKET. Please refer to *Technical Standards — Applications > Application Systems Support > Test System Management* for procedures related to these standards.

Test jobs executing in ZEKET will follow the same standards as production jobs with the exceptions described below. Please refer to *Technical Standards — Applications > Application Testing > Test/Production Updates* for standards related to the creation and scheduling of production jobs.

3.4.2.1 Requirements for Test Jobs within ZEKET

- Last character of the jobname must be an "$" or "#". Medicare Systems may use these characters as well as an "@" sign in the third or fourth position of the jobname. (The Scheduling staff is to identify the job as a test job that should be loaded into the test ZEKE scheduler uses this.)
- USERID must be an authorized test USERID, such as AMMSTST, AMMSTS2, etc. The use of production USERIDs is not allowed.
- Job class must be 'CLASS=8'.

- Test jobs must be migrated through the Endevor environment, and the jobdeck will be written to the ZEKE scheduling library, BC.SCHD.ZEKE.JCLLIB, when the jobdeck is moved to the Endevor production environment.
- DOCULIBS are required for each job.
- On call support group must be setup in the TSO Toolbox. See group TCG for an example.
- Submit the Service Request TESTPCL from the TSC Self-Service Portal.

Submit the Service Request TESTRESTART from the TSC Self-Service Portal for restarting test cycle jobs.

3.5 z/OS System Log

z/OS system logs (syslogs) are backed up daily, and are retained for 60 days.

3.6 Unix System Services

Unix System Services (USS) is a UNIX-based environment that runs under the HOST z/OS operating system. USS has limitations surrounding reliability, security, and scalability that are overcome by the z/OS operating system environment. Because of these limitations, USS should be used to support third-party software currently being used by BlueCross BlueShield of South Carolina that requires the use of USS. In addition, any new third-party software or other program that requires the use of USS should be avoided when a viable alternative exists. USS should also never be directly exposed to the network through a Secure Shell (SSH) interface. New uses of USS must be authorized by the AVP of I/S Operations.

Chapter 4 Appliances

IN THIS CHAPTER

This chapter contains standards that are applicable to the appliances used at BlueCross BlueShield of South Carolina.

4.1 DataPower Standards

DataPower is a hardware appliance supplied by International Business Machines (IBM) to simplify, secure, and accelerate service-oriented architecture.

DataPower is the centralized point of consumption for all web services. The device masks infrastructure complexity from service consumers by serving the following functions:

- Authentication — Verifying a service consumer is who they claim to be.
- Authorization — Verifying a service consumer is permitted to consume a service.
- Auditing — Tracking who called what service, when, and what the outcome was.
- Augmentation — Adding information to or removing information from a service call to satisfy some business requirement.
- Endpoint Management — Looking up and routing a service call to the correct service.
- Activity Reporting — Logging statistical service information to a data store.

DataPower devices are deployed in the DMZ and messaging networks for Commercial, PGBA and Medicare. The devices in the messaging networks facilitate web-service traffic routing by joining the Corporate, Host, and DMZ networks.

Issues or questions about DataPower may be submitted via email to DP.ADMIN.

Chapter 5 Middleware

IN THIS CHAPTER

This chapter contains standards that are applicable to the middleware used at BlueCross BlueShield of South Carolina.

5.1 MQ Standards

5.1.1 Overview of MQ

IBM Websphere MQ is used as middleware to provide reliable application integration by passing messages between applications. It allows independent and potentially non-concurrent applications across various platforms to communicate with each other.

5.1.2 MQ Usage

Queues may only be used for the following purposes:

- To facilitate the near time process.
- To put and get messages across computing platforms.
- To put messages to and get messages from entities outside of the company.

New queue requests require Enterprise Architect approval.

5.1.3 MQ Security Standards

Access to MQ objects may only be granted through domain groups for applications. Individual user IDs can then be added to the domain groups as needed. The application domain groups may only have access to the MQ objects required by the application. These objects will be identified by the Websphere MQ queue manager name and the application ID within the object name.

Administrator accounts may not be granted authority to access MQ.

5.1.4 Coding Standards for Application Use of MQ

Any application utilizing Websphere MQ must adhere to the following standards:

1. Have a code walkthrough of their MQ code with Tech Support MQ Admin before access can be granted. The program must be approved before utilization of the MQ environment.
2. Configurations concerning Websphere MQ cannot be hard coded within an application.
3. For applications that receive messages from a platform other than the platform that the application is running on, the get message with convert option (GMO_CONVERT) must be used when retrieving a message.
4. Perform error handling after each MQ call.
5. Applications that utilize a client connection to connect to a MQ environment must use a DNS name, if available, for its connection setting and secure the client connection with Secure Socket Layer (SSL). Otherwise, the IP address should be used.
6. Applications that utilize client connections when performing a MQGET, must issue a MQGET utilizing the browse first option.
7. Messages may not reside on a queue for more than one business day. Websphere MQ is not a long-term data repository.

5.1.4.1 Persistence versus Non-Persistence

A message queue should be defined as persistent under the following circumstances:

- The message is to be sent to an external queue manager.
- The message is being received from an external queue manager.
- The message is being put to a queue from a customer entering the information via a Customer Information Control System (CICS) transaction, and this information has not been written to another recoverable resource.

5.1.5 Coding Standards Specific to Host Computing Platform

5.1.5.1 Accessing MQ

On the Enterprise Server, all access to message queues is via dynamic calls to MQIP-INTERFACE: the MQ API module TS99L800. Native IBM message queue calls are not allowed. Refer to *Procedures & Tools > Host Tools > Developer Tools > Application Interfaces & Utilities* for further information.

The only exception to this standard is for DB2 triggers and DB2 stored procedures, which must use the DB2-supplied user function. Refer to *Technical Standards — Applications > File Design > Enterprise Server – DB2* for additional information.

5.1.5.2 WebSphere MQ/ACEs Monitoring

The application queue(s) must have a CICS monitor application. The Monitor must be able to perform the following tasks:

Show the Queue name, the message depth and the open input and open output counts.

- Be able to turn on and off the trigger control attribute if the Websphere MQ queue is triggered.
- Browse a message in a queue, displaying part or the entire message and message ID, correlation ID.
- Re-queue a message to an error queue.

5.1.5.3 CICS Transactions

CICS transactions that are triggered by Websphere must interrogate the MQIP-GET-BACKOUT-COUNT to determine if the message just retrieved had been previously backed out. Using this counter will help prevent trigger loops.

5.1.5.4 Request/Response Message Processing

The requesting program puts the message on the queue; MQ supplies the requesting program with the 24 byte unique Message ID. This Message ID is placed into the GETTING correlation ID field in the GET response message portion of the program. The responding program would GET the message, and when the responding program is to PUT the response to the requesting program, it is the responding program's responsibility to move the GETTING message ID to the PUTTING correlation ID and PUT the response to the queue.

5.1.5.5 Variable Length Messages

Since the actual message length of an MQ message will always be calculated by the putting application, only the number of bytes containing actual data should be put on the queue. Do not put blanks or low values in a message unless they are an integral part of the message. Blanks or low values at the end of a message should always be removed before putting the messages on the queue. MQ does not compress messages, so calculating the true message length is incumbent upon the application to keep the unnecessary data traffic and wasted pageset space to a minimum.

5.1.5.6 Queue Naming Conventions — Host

QLocal — Host

Queue names must consist of the application's system ID prefix, and the application-defined section.

```
SSSS                XXXXXXXXXXXXXXXXXXXXXXXX

|                   |

|                   |__ Application Defined Section (24 character max)

|

|__ System ID Prefix (Four (4) character max)
```

Example: WMSI.INFORM.UPLOAD

QALIAS & QREMOTE — Host

Queue names must consist of the application's system ID prefix, the recipient application's system ID prefix and the application-defined section.

```
SSSS                ZZZZ         XXXXXXXXXXXXXXXXXXXXXXX

|                   |            |

|                   |            |__ Application Defined Section (24 character max)

|                   |

|                   |__ Recipient Application System ID Prefix (Four (4) character
max)

|

|__ System ID Prefix (Four (4) character max)
```

Example: TC01.WMSI.INFO.INFORM.UPLOAD

5.1.6 Coding Standards Specific to Computing Platforms Other Than Host

Applications that utilize Java Messaging Service (JMS) must not send the JMS header when sending messages.

Applications must perform a close and disconnect from the MQ environment during every normal and abnormal end of processing.

If an application is utilizing "units of work," a MQ commit or backout must be performed to properly release MQ resources. Unless the message is part of a transaction or a group of messages, each unit of work should consist of 1 message.

When performing a MQGET, applications that utilize client connections must issue a MQGET utilizing the "browse first" option.

5.1.6.1 Queue Naming Conventions — Non-Host

QLocal — Non-Host

Queue names must consist of the queue manager name, the application's system ID prefix, and the application-defined section.

```
QQQQQQQQQQ            SSSS                  XXXXXXXXXXXXXXXXXXXXXXX

|                     |                   |

|                     |                   |__ Application Defined Section (24
character max)
```

```
|                  |

|                  |__ System ID Prefix (Four (4) character max)

|

|__ Queue Manager (10 character max)
```

Example: TC01.WMSI.INFORM.UPLOAD

QALIAS & QREMOTE – Non-Host

Queue names must consist of the queue manager name, the application's system ID prefix, the recipient application's system ID prefix and the application-defined section.

```
QQQQQQQQQQ            SSSS                  ZZZZ        XXXXXXXXXXXXXXXXXXXXXXXX

|                  |                  |           |

|                  |                  |           |__ Application Defined Section
(24 character max)

|                  |                  |

|                  |                  |__ Recipient Application System ID Prefix
(4 character max)

|                  |

|                  |__ System ID Prefix (4 character max)

|

|

|__ Queue Manager (10 character max)
```

Example: TC01.WMSI.INFO.INFORM.UPLOAD

5.1.7 Requesting New Websphere MQ Environments

Requests for new Websphere MQ environments should be sent to the email account MQ-ADMIN and include the following information:

1. *Implementation Dates*. Specify the application implementation dates for each development stage and the desired Websphere MQ Environment.

2. *Message Flow Diagram*. This diagram will show a message's path within the requested Websphere MQ Environment. The diagram will include:

   - The server(s) or guest(s) or host queue managers.
   - The queue managers and the queues to which the application will be sending messages.
   - The queue managers and the queues from which the application will be receiving messages.
   - The application portion of the queue name.

3. *Websphere MQ Usage Document*. This document will list the usage information for each queue the application will use. This information will include:

   - The expected size of each message.
   - The number of messages expected to process (e.g., daily, weekly, monthly, etc.).
   - Message frequency (e.g., consistently throughout the day, or in spurts).
   - Expected time of high volume or the peak volume time.
   - If messages should be persistent (recoverable).
   - Is the message expiring? If so, what is the time of expiry?
   - The purpose of the queue.

4. *Availability Statement*. This statement will indicate the uptime and the failover requirements for the requested Websphere MQ environment.

5.1.8 Secured Sockets Layer (SSL)

1. All channel transport types are specified as TCP/IP using Secured Sockets Layer (SSL) .
2. Production implementation uses a Public Key Infrastructure (PKI) certificate for authentication from a Certifying Authority approved by BlueCross from a Department of Defense (DoD) PKI Root Certificate Authority list.
3. Test implementations may use a "self-signed" PKI certificate.
4. All PKI certificates are stored in RACF.
5. The use of a "null" operand or 40-bit encryption is not permitted in the TELNETPARMS ENCRYPTION statement (e.g., SSL_NULL_Null, SSL_NULL_MD5, SSL_NULL_SHA, SSL_RC4_MD5_EX, or SSL_RC2_MD5_EX).
6. All channels that connect a BlueCross Enterprise Server to another BlueCross Enterprise Server have a SSL cipher specification of NULL_MD5. All other channel specifications will use DES_SHA_EXPORT.
7. A RACF DIGITAL CERTIFICATE/KEYRING form from the email conference SECURITY.FORMS must be completed and sent to RACF.ADMIN for all channel security requests.
8. All channel requests require four (4) weeks notice prior to Implementation.
9. Client Connection to E-server

   a. The Client connection and the Server connection will be defined with the name of the connecting application box name as the name of the channel, to a maximum of 20 characters (e.g., A70JUSTBECAUSEITFITS).
   b. The Server connection channel will NOT be running with a RACF supplied ID in the MCAUSERID field of the Server connection channel.
   The application will be running under the RACF supplied ID.
   c. The Server connection channel will be defined with Secured Socket Layers (SSL). The connecting application will connect with SSL.

d. The E-server application that delivers response messages to the Clients' request messages must have an EXPIRY time set equal to the Clients' wait time.
e. All applications that utilize client connections when performing a MQGET must issue it with a browse first.

5.2 Connect:Direct (Formerly NDM)

Connect:Direct is a product that moves all types of data. It manages high-performance transfers by providing user-friendly automation, checkpoint/restart error recovery and security. Connect:Direct supports SNA and TCP/IP communications protocols. At BlueCross BlueShield of South Carolina (BlueCross) though, the protocol used most is TCP/IP. Connect:Direct runs on a variety of operating systems including z/OS, Windows, AIX, and Linux. Information Communication Technology (ICT) Host Technical Support is responsible for the installation and configuration of Connect:Direct on z/OS. ICT Middleware Services is responsible for the installation and configuration of Connect:Direct on all other platforms.

For information on using Connect:Direct at BlueCross, refer to *Technical Standards – Applications > Application Development Support Tools > Naming Conventions > Job Names*.

Chapter 6 User Interfaces

IN THIS CHAPTER

This chapter contains standards that are applicable to the infrastructure for workstations used at BlueCross BlueShield of South Carolina (BlueCross).

6.1 Terminal Productivity Executive (TPX)

Terminal Productivity Executive (TPX) allows users to sign on to multiple applications from a single TN3270 window and allows users to easily toggle between these sessions. At BlueCross, Information Communication Technology (ICT) Host Technical Support installs the TPX product on the IBM E-Server (mainframe), as new releases are available from the software vendor.

6.2 z/OS Communications Server

The z/OS Communications Server is a component of the IBM z/OS operating system on the mainframe. The role of this component is to provide TCP/IP and Systems Network Architecture (SNA) network access to applications on z/OS, which allows them to communicate with partner applications on the same system, different systems within our data center, and across outside networks. The z/OS Communications Server includes common applications such as FTP for file transfer and TN3270 for host application access. The z/OS Communications Server is maintained by ICT Host Software.

6.3 Workstation Hardware/Software Determination

All hardware and software that is not published on the corporate standard hardware/software list must be sent to the ISSC Workstation Infrastructure Sub Committee (WISC) for technical review prior to ordering the product. The WISC monitors requests for new hardware for the physical workstation environment and software products that result in a change to the BlueCross physical and logical workstation environments. Refer to *Systems Architecture* > *Workstation Hardware/Software Procedures* > *Requesting Workstation Hardware/Software* for further details.

The WISC will review the technical requirements for the product to ensure that it is compatible with the corporate standard environment. Upon initial approval by both the WISC and the requester, the purchase requisition will be processed. When the product is received, the WISC will oversee the execution of a test plan to evaluate the product and its compatibility with the existing platform.

The WISC has developed test plans for the arrival of new hardware (physical environment) and software (physical and logical environment). These test plans are used to ensure consistency and completeness of all hardware and software testing.

Hardware Testing (Physical Environment)

During hardware testing, the WISC determines if the hardware works on all supported operating systems and verifies acceptable performance and functionality from within each platform.

Software Testing (Physical and Logical Environment)

For software testing, the WISC will verify that the application does not present any compatibility issues with approved software currently running on the corporate standard image. The WISC will also verify and document any possible operating system- or application-related security breaches presented by the new application. The WISC will work with the requester to test the functionality of the application, and the requester will be asked to complete a Product Evaluation Form providing written sign-off of their acceptance of the new application.

NOTE A risk assessment will be done for all new hardware and software requests.

6.4 Workstation Hardware/Software Standards

All standard workstation equipment is available through I/S Procurement and is listed in the IT Catalog on My e-Work.

All standard supported software is listed in the System Master Index (SMI) maintained by Systems Architecture.

6.5 Workstation Sanitization

For the purposes of this section, **electronic media** is any data storage device connected to workstations, printers, multi-functional peripherals or any other computer device. **Sanitization** is a procedure used by Workstation Support to render any information stored on electronic media unreadable.

For the Medicare Line of Business, any BlueCross-owned or managed electronic media must be sanitized by reformatting the device in a secure manner or by using an approved wipeout utility before it is surplussed. Diskettes and other magnetic storage media that contain any BlueCross data or software must be sanitized when they are no longer needed. Portable media may be destroyed or it may be reused after sanitization. Simply deleting a file is not sufficient to prevent someone from undeleting the file later.

Data located on all electronic media sent outside of BlueCross for repair or data recovery should be protected from disclosure by contract with the company performing the service. If a non-disclosure agreement does not exist, then the electronic media of the equipment is removed prior to shipping.

All information regarding sanitization or destruction must be maintained for a minimum of five years. The Workstation Support area will perform the sanitization procedure on any electronic media in the following situations:

- Discarding electronic media due to end-of-life or breakage
- Upon manager request

6.6 Malicious Software Protection

All workstations must include a software product that prevents both the installation of and execution of unapproved software. The approved listing of software is maintained on the SMI. Please refer to *Systems Architecture* > *General Architectural Standards* > *System Master Index* for details.

6.7 Approved Mobile Code Technologies for Workstations

Various mobile code technologies are approved for use on workstations at BlueCross and its subsidiaries such as Palmetto GBA, PGBA, CGS, etc. Mobile code types approved for use are listed in the SMI.

To ensure that these various mobile code types are not used in a malicious manner, each type adheres to corporate standards that ensure the most secure and up-to-date version is used.

Mobile code types are packaged and deployed to all workstations by ICT NH Change Deployment. Security, monitoring, scanning and deployment tools are used to enforce compliance and ensure that standards are met.

6.8 Workstation Protection

To ensure that software patches, virus protection and other software updates are kept up to date, desktop computers need to remain connected to the network and powered on. When they are not in use, the *Restart* feature should be used instead of *Log Off* or *Shut Down*. This applies to all in-office desktop computers, including those in training rooms and test labs, as well as work-at-home computers. When a work-at-home computer is restarted, it must remain connected to the Internet but disconnected from Citrix, VPN, or cmsvirtualoffice.bcbssc.com.

All corporately-owned laptop computers that are not taken home must remain connected to the network and powered on. When they are not in use, the *Restart* feature should be used instead of *Log Off* or *Shut Down*. The laptops must be secured to the desk with a serviceable locking cable to prevent theft.