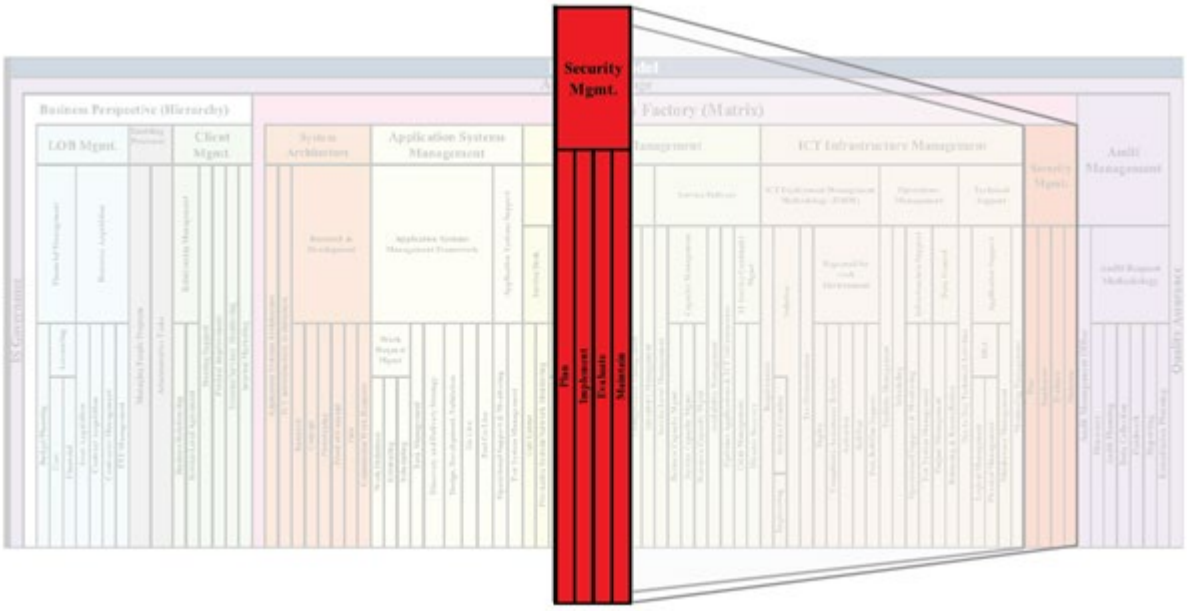
South Carolina

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

imagination to Implementation i2 INFORMATION TECHNOLOGY

Security Management



Information Systems Standards Manual

Table of Contents

Table of Figures

List of Tables

Chapter 1 Information Security Management

1.1 Incident Response

1.1.1 Incident Response Plan

1.1.2 Incident Response Controls

1.2 Security Roles

1.2.1 Data Security Department

1.2.2 System Security Officer or Contact

1.3 Security Framework Concepts

1.3.1 National Automated Clearing House Association

1.3.2 National Institute of Standards and Technology

1.3.3 NIST Control Families

1.4 Application and Data Security Control Standards

1.4.1 Authorized Access and Use of Selected Systems for Qualified Users

1.4.2 Resource Access Control Facility

1.4.3 Identity Management Standards: Security Group Objects

1.4.4 Cloud Identity and Access Management Standards

1.4.5 Data Security Standards

1.4.6 Applications/Software System Security Control Standards

1.4.7 Security below the Transaction Level

1.4.8 External Security Directive

1.4.9 Application Security Evaluation

1.4.10 User Session Configuration and Termination

1.5 Configuration and Vulnerability Management

1.5.1 Patch Implementation/Vulnerability Remediation Schedule

1.5.2 Configuration Remediation Schedule

1.6 Threat Management

1.6.1 Information Security Vulnerability Management Process

1.7 Malicious Code Protection

1.8 Windows Server Security

1.8.1 Commercial Windows Server Security Configuration

1.8.2 Security Assessment and Authorization

1.8.3 Planning

1.8.4 System and Services Acquisition

1.8.5 Technical Class

1.8.6 Operational Class

1.8.7 Configuration Management

1.8.8 Maintenance

1.8.9 Alternate Platform Administrative Procedures

1.9 Risk Assessment

1.9.1 Operation Risk Management

1.10 Medicare Considerations

1.10.1 Medicare Support Definition

1.10.2 Portable Electronic Media Information Transfer

1.10.3 ARS Control Family Policy and Procedures

1.11 Certificates and Public Key Infrastructure

1.11.1 Definitions and Summary

1.11.2 Certificate Authorities

1.11.3 Certificate Categories and Use Cases

1.11.4 Certificate Keys

1.11.5 Certifcate Inventory Management

1.12 Production Data Updates by I/S Personnel

1.13 Personnel Security

1.13.1 Personnel Screening

1.14 Awareness and Training

1.14.1 Security Awareness and ComplianceTraining

1.14.2 Professional Training

Chapter 2 System Security

2.1 System Administrator Access

2.1.1 System Administrator Active Directory (A Dash) Accounts

2.1.2 System Administrator Responsibilities

2.1.3 System Administrator Standards

2.1.4 Requesting System Administrator Access

2.1.5 Removal of System Administrator Access

2.1.6 Periodic Reviews

2.2 Cloud Administrator Access

2.2.1 Requesting Cloud Administrator Access

2.2.2 Removal of Cloud Administrator Access

2.2.3 Authenticating Cloud Administrator Accounts

2.3 Management Class

2.3.1 Organizational Security Program Management

2.3.2 Access Control

2.3.3 Audit and Accountability

2.3.4 System and Communications Protection

2.3.5 System and Information Integrity

2.3.6 Access and Security

2.3.7 Secure FTP – Security Option for the FTP Clients

2.4 Security Systems

2.4.1 Authentication, Authorization and Accounting

2.4.2 Encryption

2.4.3 Endpoint Protection/Malware Protection

2.4.4 Enterprise Security Event Logging and Management

2.4.5 Firewalls

2.4.6 Internet Traffic Filter

2.4.7 Intrusion Detection (Network and Host Based)

2.4.8 Public Key Infrastructure

2.4.9 Remediation, Patch and Configuration Management

2.4.10 Virtual Private Network

2.4.11 Vulnerability Scanners and Management Systems

2.4.12 Data Loss Protection

2.4.13 Cloud Image Management

Chapter 3 Application Security

3.1 RACF Security Coding Procedures

3.1.1 Procedures to Query RACF Security

3.1.2 Security Application Coding Examples

3.1.3 Application Level Security Tables

Table of Figures

Figure 1-1 Prefix Diagram

Figure 1-2 File Access Diagram

Figure 1-3 Printer Access Diagram

Figure 1-4 Application Access Diagram (AD)

Figure 1-5 Application Access Diagram (Azure)

Figure 1-6 Device Access Diagram (AD)

Figure 1-7 Device Access Diagram (Azure)

Figure 1-8 Delivery Diagram (AD)

Figure 1-9 Delivery Diagram (Azure)

Figure 1-10 UNIX Access Diagram

Figure 1-11 Certificate Management — Managing New, Existing and Revoked Certificate Inventory

Figure 1-12 Certificate Management — Managing Certificate Ownership and Accountability

Figure 2-1 BlueCross Warning Statement

Figure 2-2 RACF Password Warning Used to Access VTAM

List of Tables

Table 1-1 Management Control Families

Table 1-2 Technical Control Families

Table 1-3 Operational Control Families

Table 1-4 Password Syntax Requirements

Table 1-5 Daily File Criteria for Existing Role-Based Group

Table 1-6 Cloud Shared Responsibility Model

Table 1-7 Corporate and Commercial Patch Maintenance and Remediation

Table 1-8 PGBA Patch Maintenance and Remediation

Table 1-9 Medicare Patch Maintenance and Remediation

Table 1-10 Medicaid Patch Maintenance and Remediation

Table 1-11 Corporate and Commercial Configuration Remediation

Table 1-12 PGBA Configuration Remediation

Table 1-13 Medicare Configuration Remediation

Table 1-14 Line of Business Documents

Table 1-15 Version Record Example

Table 2-1 Technology System Administrator Definitions

Table 2-2 Approved AAA Products

Table 2-3 Approved Endpoint Protection Products

Table 2-4 Approved Log and Security Event Management Products

Table 2-5 Approved Firewall Products

Table 2-6 Approved Internet Filter Products

Table 2-7 Approved Intrusion Detection Products

Table 2-8 Approved Intrusion Detection Products

Table 2-9 Approved Remediation, Patch and Configuration Products

Table 2-10 Approved VPN Products

Table 2-11 Approved Vulnerability Scanning Products

Table 2-12 Approved Data Loss Protection Products

Table 3-1 Query Security RESTYPE Values

Chapter 1 Information Security Management

1.1 Incident Response

The following section defines how the organization shall:

- Establish an operational incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to appropriate organizational officials or authorities or both.

1.1.1 Incident Response Plan

The I/S organization of BlueCross BlueShield of South Carolina and any affiliates or subsidiaries it directly or indirectly controls (BlueCross) follows the established Incident Response Plan (IR Plan) document that is maintained by the Cybersecurity Operations (SecOps) team. The SecOps team works with the appropriate areas within the I/S organization to research corrective actions to contain and eradicate the threat.

1.1.2 Incident Response Controls

BlueCross has a formal incident response team established for systems and operations recovery procedures. Incident response teams and contacts are documented in the Corporate IR Plan. BlueCross also has documented plans and procedures for responding to a computer security incident. A security incident response is a collaboration of individual users, the Compliance department, and security specialists (network, Enterprise Server, and facilities areas).

The following controls exist to identify and report incidents:

- Security incident procedures
- Report procedures
- Response procedures
- Procedures to regularly review records of information system activity, such as security incident tracking reports
- Process to modify incident handling procedures and control techniques after an incident occurs

All violations, including potentially hazardous activities, are summarized and reported to I/S Senior Management as soon as possible. If a suspected or actual security incident has occurred, employees are trained to notify their immediate supervisor or manager on first noticing a possible security incident. Immediately after observing a suspected information security incident, employees are to contact the Technology Support Center (TSC), and a ticket will be generated to initiate the Corporate IR Plan.

The SecOps team monitors several tools, such as the Security Information and Event Management system (SIEM), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Host-based Intrusion Detection System (HIDS), Firewall logs, Antivirus consoles, etc., to look for anomalies that indicate suspicious activity.

1.2 Security Roles

The Data Security Department of BlueCross BlueShield of South Carolina (BlueCross) Information Systems (I/S) Division and the Business System Security Officers (SSOs) assist the I/S organization in the recommendation, administration and review of applicable security controls designed to protect the corporation from threats and vulnerabilities. The actions of these areas are based on the concept of balancing the potential losses due to known or suspected threats and vulnerabilities against the costs associated with containment of the risk.

Any I/S related technical standard that applies to the security functions performed by these roles is documented within this chapter of the ISSM.

The following describes each of these roles.

1.2.1 Data Security Department

The Data Security department is responsible for assisting in the review and identification of needed security controls, the administration of established system security end-user controls, and the reporting of security incidents.

A primary method of identifying and eliminating potential security control issues is accomplished through participating in the System Development Life Cycle process as described in the Application Systems Management Volume.

When any waiver to the security standards is granted through the standard waiver process, the appropriate individuals within the I/S Security Organization will be notified.

1.2.1.1 Data Security Administration

Data Security Administration is responsible for the day-to-day security operations of access control software within multiple security architectures and within multiple secure applications. Data Security ensures requirements are met that are set forth in BlueCross BlueShield of South Carolina's security policies, standards and procedures.

1.2.2 System Security Officer or Contact

Each Line of Business (LOB) within the organization designates an individual to be the primary contact to manage the Information Security program, ensure the implementation of necessary safeguards, and coordinate applicable security control reviews.

The System Security Officers (SSOs) and/or System Security Contacts (SSCs) will interact with applicable LOB business management, I/S, and the Security Council to organize and conduct security reviews and Risk Assessment activities. They are also responsible for assisting in the review and identification of needed security controls for their LOB systems and the reporting of security incidents.

A proactive method of identifying and eliminating potential security control issues is accomplished through participating in the System Development Life Cycle process as described in the Application Systems Management Volume.

1.3 Security Framework Concepts

1.3.1 National Automated Clearing House Association

National Automated Clearing House Association (NACHA) Operating Rules are Automated Clearing House payment standards that define the roles and responsibilities of financial institutions and establish guidelines for each network participant.

1.3.2 National Institute of Standards and Technology

National Institute of Standards and Technology (NIST) has developed the special publication NIST 800-53, which provides a catalog of security and privacy controls that are designed to be tailored for use by many businesses.

The NIST 800-53 controls have been utilized and tailored to create the following frameworks or security guidelines and many more:

- **CMS MARS-E** — Minimum Acceptable Risk Standards for Exchanges that are used with Medicaid.
- **CMS ARS** — Acceptable Risk Safeguards that are used for Medicare MAC contracts.
- **NIST 800-171** — A publication that defines the protection of unclassified federal information in nonfederal systems and organizations that is used for PGBA contracts.
- **BlueCross Corporate Security Framework** — The set of 19 corporate security policies to be used by BlueCross BlueShield of South Carolina and any affiliates or subsidiaries it directly or indirectly controls (BlueCross).

1.3.3 NIST Control Families

The NIST 800-53 controls are organized into control families and classes for ease of use in the control selection and specification process. There are three general classes of security policies and controls (Management, Technical, and Operational) and over 20 control families. Each family contains security policies and controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family.

The following are the 18 control families selected for inclusion in the BlueCross Corporate Security Framework grouped by their general class.

1.3.3.1 Management Control Families

Management control families (Table 1-1) are the security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Management Control Families

Control Family	Definition	Intent
Program Management (PM)	Develop and promote formal, documented policies and procedures governing the minimum-security requirements and ensure their effective implementation.	To ensure that policies and procedures are defined so that appropriate security measures are in place and are effectively implemented.
Planning (PL)	Define and implement security plans that describe the security controls in place or are planned and define the rules of behavior for individuals.	To ensure that a process is in place to maintain and update the security posture of the organization.
Security Assessments and Authorization (CA)	Assess the security controls, develop and implement plans of action designed to correct deficiencies and eliminate vulnerabilities, authorize the operation of information systems, and monitor effectiveness of information system security controls.	To ensure that processes are in place to assess the security posture of the organization to ensure that it is being maintained properly and effectively.
Risk Assessments (RA)	Assess the risk to operations, assets, and individuals, resulting from the operation of information systems and the associated processing, storage, or transmission of information.	To ensure that processes are in place to allow the organization to understand risks to the company.
Systems and Services Acquisition (SA)	Allocate sufficient resources to protect organizational information systems, employ system development life cycle processes that incorporate information security considerations, employ software usage and installation restrictions, and ensure that third-party providers employ adequate security measures.	To ensure that the organization is not compromised through third-party software or services.
Supply Chain Risk Management (SR)	Identifying, assessing, and mitigating the risks to the integrity, trustworthiness, and authenticity of products and	To ensure that supply chain risks are managed effectively and that the supply chain can

Management Control Families

Control Family	Definition	Intent
	services within the supply chain.	continue to operate smoothly.

Table 1-1 Management Control Families

1.3.3.2 Technical Control Families

Technical control families (Table 1-2) are the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Technical Control Families

Control Family	Definition	Intent
Access Control (AC)	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices and to the types of transactions and functions that authorized users are permitted to exercise.	To ensure that processes are in place that allow people access to only the information that they need.
Audit and Accountability (AU)	Create, protect, and retain information system audit records to enable the monitoring, analysis, investigation, and reporting of inappropriate information system activity so that individuals can be held accountable for their actions.	To ensure that data is created and kept so that in allows bad actions to be identified and traced to the person responsible.
Identification and Authentication (IA)	Identify information system users, processes acting on behalf of users, or devices and authenticate the identities of those users, processes, or devices, as a prerequisite to allowing access to information systems.	To ensure that people that access the system have appropriate authorization and that the actions that they take are identified.
System and Communication Protection (SC)	Monitor, control, and protect organizational communications and employ architectural designs, software development techniques, and systems engineering principles that promote effective information security.	To ensure that data entering and leaving the information system does not compromise the organization's security posture.

Table 1-2 Technical Control Families

1.3.3.3 Operational Control Families

Operational control families (Table 1-3) are the security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

Operational Control Families

Control Family	Definition	Intent
Awareness Training (AT)	Ensure that managers and users of information systems are made aware of the security risks and ensure that personnel are adequately trained to carry out their assigned, information security-related duties and responsibilities.	To ensure that people in the organization are trained with respect to security requirements and can carry out their security responsibilities.
Configuration Management (CM)	Establish and maintain baseline configurations and inventories of information systems (including hardware, software, and documentation) throughout the system development life cycles; and Establish and enforce security configuration settings.	To ensure that all components in the information system are set up and managed as expected.
Contingency Planning (CP)	Implement plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.	To ensure that processes are in place that allow the organization to effectively operate despite experiencing disruptive events.
Incident Response (IR)	Establish incident handling capability for information systems and report incidents to appropriate officials and/or authorities.	To ensure that processes are in place that allow the organization to respond effectively to security incidents.
Maintenance (MA)	Perform timely maintenance on information systems; and Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct maintenance.	To ensure that the information system is effectively maintained.
Media Protection (MP)	Protect information system media,	To ensure that processes are in

Operational Control Families

Control Family	Definition	Intent
	both paper and digital; Limit access to information system media to authorized users; and Sanitize or destroy information system media before disposal or release for reuse.	place that protect the data stored by the organization.
Physical and Environmental (PE)	Limit physical access to information systems, equipment, and operating environments to authorized individuals; Protect the physical plant; Provide supporting utilities for information systems; Protect against environmental hazards; and Provide environmental controls in facilities containing information systems.	To ensure that the buildings and computer rooms are secure and safe from unauthorized access or environmental impacts.
Personnel Security (PS)	Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; Ensure that information and information systems are protected during and after personnel actions such as terminations and transfers; and Employ formal sanctions for personnel failing to comply with security policies and procedures.	To ensure that the organization is not harmed due to individual's actions.
System and Information Integrity (SI)	Identify, report, and correct information and information system flaws in a timely manner; Provide protection from malicious code; and Monitor information system security alerts and advisories and take appropriate actions in response.	To ensure that the data stored in the information system is not tampered with or compromised.

Table 1-3 Operational Control Families

1.4 Application and Data Security Control Standards

The following security standards apply to all new development and will be retrofitted into any system or subsystem that is undergoing a major revision. These standards apply not only to the Production systems and environments, but also to those in development or validation.

Any security system utilized must:

- Identify and verify users who wish to access the system.
- Identify protected resources and the level of protection.
- Allow only authorized users to access the protected resources.
- Provide a method to administer security.

Security systems must have the ability to maintain audit trail records related to the following user and administrator's activities:

- Unsuccessful and successful access attempts
- File-related activities (Open/Delete/Modify) against sensitive information
- The success or failure to complete one of these events
- The User ID, the date/time of the event and where the event was initiated

The decision to maintain audit trails and to what level of detail should be based on:

- The value or sensitivity of data and resources affected.
- The type of environment.
- The legal and regulatory requirements.

The definition of the level of security and the audit trail to be employed will occur during the Development Life Cycle. If significant issues arise regarding a proposed level of security, they will be directed to the Chief Information Officer for final resolution.

Audit trails are backed up daily, then merged together weekly on tapes. The weekly tapes are later merged together on a monthly basis to tape, which is retained for seven years. Companion Data Services' (CDS) Electronic Data Communications (EDC) weekly tapes are also merged together on a monthly basis to a write once read many (WORM) tape, which is retained for seven years.

1.4.1 Authorized Access and Use of Selected Systems for Qualified Users

Access authorization forms are submitted to Data Security Administration via secured standard forms. The secure forms are restricted to supervisors, their designees (known as Security Points of Contact) and higher levels of management. Data Security Administration reviews the forms and obtains approval from owners/authorizing officials, if required. Approved request forms are maintained on file in an electronic database.

IBM's Resource Access Control Facility (RACF) is an External Security Manager (ESM) access control software product utilized in the mainframe environment. RACF controls entry to the system, access to datasets, and use of logical resources. Many applications use application-level security, in conjunction

with RACF, to restrict user access to specific screens or data element fields needed to perform routine job requirements.

Microsoft's Active Directory is the access control product utilized in the Windows network environment. Active Directory controls entry to the systems, access to files and use of logical resources. Many applications use application-level security, in conjunction with Active Directory, to restrict user access to specific screens or data element fields needed to perform routine job requirements.

Each qualified/authorized user is assigned a unique ID and password combination with access to use selected systems and data using the principle of least privilege. Each unique ID is placed in logical groups (role based, organization based, system based or resource based). Logical groups are configured within Access Control Systems (RACF, Active Directory, etc.) to grant the minimum resource authorizations necessary to use selected systems and data based on the job function or business need.

1.4.1.1 User IDs and Passwords

The following standard applies to all new development and any system work effort that is undergoing a major revision.

Do not include any hard-coded logic within an application program that examines and makes decisions based upon the layout and content of a RACF User ID, Operator Identification (OPID) and/or TermID. If there is a need to obtain the identity and security authorization of the user or the organization that the user belongs to, refer to *Security Management > Application Security > RACF Security Coding Procedures* for the prescribed methods to systematically retrieve the identity and security authorization of the user represented by the User ID.

Each system user shall be assigned a unique User ID to access Host and Non-Host platforms and applications.

Previously used User IDs are only reassigned to the previous owner of that User ID. Random number generator tools that consider User ID history databases are used to prevent reuse of previously assigned User IDs.

The appropriate management must complete the approved request form to request the assignment of a unique User ID for each employee, contractor and temporary employee requiring access to Host and Non-Host platforms and applications.

Temporary accounts are assigned to external auditors and vendors. Each temporary account is configured with a fixed duration not to exceed the time period specified by the requestor. The termination date must not exceed 30 days for temporary accounts defined on Medicare platforms.

User IDs may be revoked, disabled, or deleted at any time at the discretion of a Data Security Manager based upon concerns regarding security violations. When a User ID is revoked, disabled or deleted, a Data Security Manager will contact the system user's management chain regarding the issues or concerns.

The composition of each User ID will be determined by Data Security Administration and will consider interface requirements for existing applications.

Certain applications contain hard-coded logic that interprets the spelling of the User ID to determine the security profile information regarding the user. When establishing new User IDs, Data Security Administration will take this existing logic into consideration.

User IDs will be:

- Revoked or disabled when not used for 30 or more days.
- Deleted when not used for 90 or more days.
- Revoked or locked when an incorrect password is entered three consecutive times.
- Configured to require a password change every 30 days.

To prevent reuse of previously used passwords, passwords will be stored for a minimum of twelve prior generations. RACF and Active Directory systems have been configured to enforce User IDs to have a one (1)-day minimum password age.

User IDs are configured to require strong passwords. The password syntax requirements are below in Table 1-4 on the next several pages.

Password Syntax Requirements

Platform	Password Length (Minimum)	Password Length (Maximum)	Password Must Contain
Host (RACF [z/OS & z/VM] — Corporate)	8	8	• At least one alpha character • One numeric character • One of the following special characters: @ # $
Host (RACF [z/OS] — Medicare)	8	8	• At least one uppercase alpha character • At least one lowercase alpha character • One numeric character • One of the following special characters: @ # $ • Change at least four of the eight characters from your previous password (Changing a **p** to a **P** is not considered a character change.) • No more than three consecutive characters can remain unchanged from your previous password • No repeating characters are allowed in the password • The User ID cannot be

Password Syntax Requirements

Platform	Password Length (Minimum)	Password Length (Maximum)	Password Must Contain
			contained in the password • The username cannot be contained in the password • Sets of specific character strings are not allowed in the password
Host (RACF [z/VM] — Medicare)	8	8	• At least one uppercase alpha character • At least one lowercase alpha character • One numeric character • One of the following special characters: @ # $ • Change at least four of the eight characters from your previous password (Changing a **p** to a **P** is considered a character change.)
Host (RACF [z/OS & z/VM] — VDC)	8	8	• At least one alpha character • At least one numeric character • At least one of the following special characters: @ # $
Non-Host (Active Directory — Corporate)	8	128	• At least one from three of the four categories: ○ Lowercase alpha character ○ Uppercase alpha character ○ Numeric character ○ Non-alphanumeric (special) characters: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /
Non-Host (Active Directory — Medicare)	8	128	• At least one lowercase alpha character • At least one uppercase alpha character • One numeric character • One of the following nonalphanumeric (special)

Password Syntax Requirements

Platform	Password Length (Minimum)	Password Length (Maximum)	Password Must Contain
			characters: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /
Non-Host (Active Directory — Medicare Administrator Accounts)	15	128	• At least three lowercase alpha characters • At least three uppercase alpha characters • At least three numeric characters • At least three of the following nonalphanumeric (special) characters: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? / • Must not be or contain the account • Must not be or contain the username
Non-Host (Active Directory — VDC)	16	128	• At least three numeric characters • At least three uppercase alpha characters • At least three lowercase alpha characters • At least three of the following nonalphanumeric (special) characters: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /

Password Syntax Requirements

Platform	Password Length (Minimum)	Password Length (Maximum)	Password Must Contain
Non-Host (Active Directory — PGBA)	15	128	• At least two numeric characters • Two uppercase alpha characters • Two lowercase alpha characters • Two of the following nonalphanumeric (special) characters: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /
Non-Host (Active Directory — Companion Life [CLife] Subsidiaries	14	128	• At least one from three of the four categories: ○ Lowercase alpha character ○ Uppercase alpha character ○ Numeric character ○ Nonalphanumeric (special) character: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /
Oracle — Corporate	8	30	• One lowercase alpha character • One uppercase alpha character • One numeric character • One of the following nonalphanumeric (special) characters: ~ ! # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /
Oracle — Medicare	8	30	• One lowercase alpha character • One uppercase alpha character • One numeric character • One of the following nonalphanumeric (special) characters: ~ ! # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /
Oracle — VDC	15	30	• At least two numeric characters

Password Syntax Requirements

Platform	Password Length (Minimum)	Password Length (Maximum)	Password Must Contain
			• At least two uppercase alpha characters • At least two lowercase alpha characters • At least two of the special character: #
Oracle — PGBA	15	30	• Two lowercase alpha characters • Two uppercase alpha characters • Two numeric characters • Two of the following nonalphanumeric (special) characters: ~ ! # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /

Table 1-4 Password Syntax Requirements

RACF passwords are stored in an encrypted format using the Key Derivation Function Advanced Encryption Standard (KDFAES) algorithm.

Windows and UNIX®[1] password files are encrypted at the server level for security.

The above Password and User ID standards apply to direct user interaction with Enterprise Server applications. Application to application password and User ID requirements, if any, will be documented within the ISSM based on the platform of the calling application.

Data Security Administration will use the legal name as stored in the HR system when creating or modifying User IDs on any target system. This standard applies to the name field of all new User IDs defined on any target system including, but not limited to, RACF, Active Directory, Email, Unix and SecurID.

System Accounts

Applications and subsystems with mechanisms that require authentication and/or authorization using a User ID are assigned system accounts on various target systems. Internal points of contact (POCs) must be identified and associated with all system accounts. System account POCs are responsible for periodic certification of system accounts, identifying required access permissions, and the timely changing of system account passwords every 60 days, when required. z/OS system accounts require two POCs: a

[1] UNIX is a registered trademark of The Open Group.

password POC and a recertification POC. A single user can fulfill both POC roles for a z/OS system account.

Data Security Administration sets non-expiring passwords on User IDs associated with a special purpose. Specific examples of this are production applications and subsystems with mechanisms that require the use of a User ID to transfer data between sites, platforms, and environments, or to access data via scheduled batch programs or web applications.

1.4.2 Resource Access Control Facility

Resource Access Control Facility (RACF) is the primary security control software for all software at the transaction level and for all data on the Enterprise Server.

All Customer Information Control System (CICS) regions shall be configured to use System Authorization Facility (SAF) to route authorization requests to the External Security Manager (ESM) RACF.

All CICS regions shall be configured to require users to identify themselves to CICS by requiring their RACF User ID and password in order for them to obtain authorization to run the transactions that they are permitted to use.

A standard (default) CICS User ID should have access only to those transactions for which security is not required, which should be limited in number.

Refer to the section *User IDs and Passwords* above for User ID and Password standards that apply to the utilization of RACF.

1.4.2.1 Access Control: Role-Based, Model-After & Template

Access to RACF-protected and Active Directory-protected information system resources will be provisioned via Role-Based, Model-After and Template methodologies.

Role-Based Access Control

Role-based Access Control (RBAC) will be used to provision access to RACF-protected and Active Directory-protected information system resources. This method of logical access control ensures automatic availability of required data/information system resources by default upon hiring/moving from one job to another.

NOTE Selected sensitive applications/systems (e.g., Human Resources) are excluded from this method of access control. Access to sensitive applications/systems will be granted at the individual User ID level.

Employees are assigned a User ID by Data Security with membership to at least four groups based on:

1. Cost Center.
2. Company, division, and job code.

3. Job code and Cost Center.
4. Customized departmental security group. *(These will be defined to identify specific job functions within a Cost Center by Data Security Administration in conjunction with the Cost Center managers.)*

NOTE Security Administration and the Resource/Data Owner will deal with individual employee access exceptions as they arise.

One of these four groups must be used in access lists.

Example:

IF USER-A…

…is a member of Company 001, Division 44, Cost Center 804; Job Code IT126; and customized departmental security group IT126SSP

…THEN USER-A…

…should be a member of access groups named CC804, A44IT126, IT126804 and IT126SSP.

These groups should be placed into the access list of I/S system resources based on the following criteria:

1. If all members of a Cost Center require access to a resource, then group CC804 should be in the access list.
2. If all members of Company 001, Division 44, Job Code IT126 require access to a resource, then group A44IT126 should be in the access list.
3. If all members of Job Code IT126 within Cost Center 804 require access, then the Group IT126804 should be in the access list.
4. If all members of customized departmental security group IT126SSP within Cost Center 804 require access, then the Group IT126SSP should be in the access list. *(This is an eight-byte field to be determined by the Cost Center manager and Data Security Administration.)*

To locate an existing employee's role-based group, search by employee ID and/or RACF User ID within dataset BC.ISEC.DAILY.CCJCFILE(0) (z/OS Corporate system) or CDS.ISEC.DAILY.CCJCFILE(0) (z/OS Medicare system). The file layout is described below (Table 1-5).

Daily File Criteria for Existing Role-Based Group

Column	Length Format	Contents
1	08 Characters	Role-based RACF group
10	08 Characters	RACF User ID (CICS/TSO)
20	20 Characters	Name from RACF database
45	04 Characters	Employee Number

Daily File Criteria for Existing Role-Based Group

Column	Length Format	Contents
50	20 Characters	Last name space First name

Table 1-5 Daily File Criteria for Existing Role-Based Group

Model-After Access Control

Model-After access provisioning requires a received request to have a valid Model-After User ID entered into the request by the submitter. All non-restricted accesses provided to the Model-After ID will be granted to the target User ID. Restricted access will need to be specifically requested.

Template Access Control

Template access will be used to provision access where such templates exist and are appropriate for the User ID.

1.4.2.2 Access Templates

Medicare company employees that use corporate/commercial systems are granted access based on pre-defined systems for each specific division and job family. Some Medicare company-specific network file and folder accesses are also granted based on pre-defined access for each division and job family. The following standard applies to this domain of users and related systems.

Access authorization to mainframe (Host) and network (Non-Host) information system supported resources will be granted using division/job family templates. Division/job family templates are pre-defined collections of RACF and Active Directory groups used to grant standard access to systems, applications and data. Employees within the same division and job family will be granted like access permissions using division/job family templates. This method of logical access control ensures automatic availability of required data/information system resources by default upon hiring/moving from one division and job family to another.

NOTE Selected sensitive and restricted applications/systems data (e.g., Human Resources, Federal Information Security [FIS], Multi-Carrier System [MCS], etc.) are excluded from this method of access control. Access to sensitive and restricted applications/systems/data will be granted at the individual User ID level.

1.4.2.3 Remote Access

In order to protect the critical systems and data that reside on our Host system, two-factor authentication is required. BlueCross BlueShield of South Carolina (BlueCross) employs the

combination of RACF and RSA SecurID token through an encrypted connection using Citrix to achieve two-factor authentication.

RSA SecurID tokens are assigned to employees and business partners who require multi-factor authentication to perform their job duties. This can include, but is not limited to, those who regularly travel on business, work-at-home (W@H) staff, and office staff.

To request an RSA SecurID token, managers or above must submit a SecurID Token Request ticket via the TSC Self-Service.

Users assigned an RSA SecurID token are required to immediately notify their manager or point of contact when tokens are lost or missing. Lost or missing tokens are disabled immediately upon notifying the TSC/Data Security Administration. SecurID tokens are disabled on the effective date when employees or business partners terminate, transfer or no longer have a job function or business need for remote access into our systems.

1.4.3 Identity Management Standards: Security Group Objects

BlueCross BlueShield of South Carolina (BlueCross) security group objects must be created and maintained in a way that permits the company to meet regulatory compliance obligations and reduce the risk of security breaches. The most basic of these requirements that span the entire corporation can be summarized in two phrases: minimum necessary and least privilege. These are defined below:

- Minimum Necessary — Take reasonable steps to limit the access to and disclosure of information to the minimum necessary to accomplish the intended purpose.
- Least Privilege — Every program and every user of the system should operate using the least set of privileges necessary to complete the job.

1.4.3.1 Security Group Objects

Security group is a security object that resides within an identity source technologoy (e.g., Active Directory, Azure, LDAP, etc.) that represents a collection of user and computer accounts, contacts, and/or other groups that can be managed collectively as a single security unit for various purposes. Security Groups have several different associated properties or attributes that prescribe how they can be used, where they can be used and what they can contain.

NOTE Certain identity source technologies may not support all general characteristics or values as specified in this section. They will be called out and addressed specifically where appropriate.

Azure Active Directory has two group types: security groups and M365 groups. Security groups are managed by administrators; M365 groups are managed by end users directly. References and standards applied to Azure Active Directory groups in this document will apply only to security groups managed by administrators and will not pertain to M365 groups.

M365 groups are created with new Microsoft (MS) Teams channels, MS SharePoint sites, and other features such as Planner. M365 groups do not contain security policies, security configurations, or

licensing. M365 group names cannot use the same naming convention as security groups, as they must be in a usable email address naming format. M365 Groups do not support nesting with other M365 Groups or with distribution or security groups.

Group Attributes

Groups have several attributes that define certain characteristics of a group that are not part of the group name. The attributes must be updated independently of the name when the group is created or modified but can be included in output or reporting data as needed.

Group Description

When creating a group, it's crucial to include specific information about its purpose and intended use for future reference. When ownership is transferred or if the group becomes orphaned, this information is used to understand why it exists and for insight into its usage.

Restricted Group

A restricted group indicates that membership changes to the group must be reviewed and approved by the Group Owner or the Group Point of Contact (Group POC). A group can be restricted for any reason This most commonly occurs when the group grants access to sensitive information, a privileged function, or a resource that would incur a cost that must be charged back to the user or Group Owner. If a group is not restricted, owner and Group POC approval are not needed to make changes to group membership.

Active Directory

The attrbitue *bcbsscRestrictedGroup* is used to denote a group as Restricted in Active Directory. This field will contain a value of True, if so, or False/NULL, if not.

Azure Active Directory

Azure Active Directory cannot use group attributes to denote Restricted and Unrestricted groups. Refer to the group naming diagrams in the subsection *Resource Control Groups* below for more information on how they are identified.

Administrative (Privileged) Group

A privileged group indicates elevated access to an application or system to perform high-level actions such as configuration changes or modifying access. A privileged group's membership is audited on an ongoing basis for security purposes. Once a group is marked as privileged, it is only allowed to contain System Administrator (A-) accounts, System/Service accounts, or other privileged groups.

NOTE If a group is identified as privileged, then it is also becomes a restricted group and should be identified accordingly.

Active Directory

The attrbitue *bcbsscAdministrativeGroup* is used to denote a group as Restricted in Active Directory. This field will contain a value of True, if so, or False/NULL, if not.

Azure Active Directory

Azure Active Directory cannot use group attributes to denote Administrative groups. Refer to the group naming diagrams in the subsection *Resource Control Groups* below for more information on how they are identified.

Group Owner

Active Directory

The Group Owner is responsible for approving group membership if it is marked *restricted* and for attesting that the permissions assigned to the group within the application or system is in accordance with the group's prescribed access. The Group Owner is also responsible for approving any group nesting if applicable.

Azure Active Directory

Notating both a group owner and a POC must occur in the Owners attribute in Azure Active Directory. More than one individual can be specified in the Owners attribute. There is no specific attribute for POC.

Group POC

Active Directory

The Group POC is a delegate of the Group Owner and may approve or deny group access, including nesting; however, the Group Owner should be included on all communication.

Azure Active Directory

Notating both a group owner and a POC must occur in the Owners attribute in Azure Active Directory. More than one individual can be specified in the Owners attribute. There is no specific attribute for POC.

Exception

Active Directory

The Active Directory attribute *bcbsscgroupattribute1* is used to identify any reviewed and approved groups that do not meet the defined naming standard in Active Directory.

Azure Active Directory

In Azure Active Directory, the first two characters of the Group Description field will start with "NE" to identify any reviewed and approved groups that do not meet the defined naming standard.

Group Name

BlueCross security group names consist of both data components and delimiters. These individual name components are structured data elements, that when combined with the delimiters, clearly define the group's type, purpose, and/or access.

Group Name Delimiter

The data elements of each group name must be separated by a standard delimiter, underscore (_), which allows the group names to be broken down into structured elements for data analysis and reporting. These characters are not allowed within the named sections and are only used for named section separation.

Resource Control Groups

A Resource Control Group is applied directly to a file system, printer, application, device or other resource and is used to permit a defined level of access for that resource.

Group Prefix

Each Resource Control Group name begins with a three (3)-letter prefix. See Figure 1-1 for a graphical representation.

1. **Resource Access Control Type** — The *first letter* represents a resource access control type.
2. **Naming Status** — The *second letter* represents the group's ability to withstand a name change without affecting downstream access, provisioning or processes. Windows-based systems rely on the use of a Security ID (SID) to identify a group and its members, which is not related to the group's actual name. Non-Windows systems and applications that rely on Lightweight Directory Access Protocol (LDAP) utilize the group's actual name to make use of it and are affected by name changes. The two options for Naming Status are as follows:
    a. **Dynamic (D)** — This letter means that the group name can be changed without affecting the members or the systems downstream that utilize the group for access. Being able to rename groups after technical changes minimizes group duplication and cleanup efforts.
    b. **Static (S)** — This letter means that the group name cannot be changed. The way that the group will be used prohibits it from being changed without affecting downstream access. This designation helps identify risk for downstream impacts in cases where a system might have a hard-coded reference to a group name for example.
3. **Nestability** — The *third letter* represents whether or not nesting is allowed. Some systems and applications cannot recognize users that are nested into a security group through another group. The two options for Nestability are as follows:
    a. **Nesting Allowed (N)** — This letter means that nesting is allowed, and other groups can be members of (nested into) this group. This should be the default choice where possible.
    b. **Flat Only (F)** — This letter means that nesting is not allowed within the group and is only used when specifically requested. Users must be added directly to these groups to successfully grant access.

	Prefix						
Char.	X		X		X		_
Element	A		B		C		
Desc.	*Resource Access Control Type*		*Naming Status*		*Nestability*		*Sep*
Options	F	File Access	D	Dynamic	N	Nesting Allowed	
	P	Printer Access	S	Static	F	Flat Only	
	A	Application Access					
	D	Device Access					
	L	Delivery					
	U	Unix Access					
Source	*RULEs*		*User Value*		*User Value*		

Figure 1-1 Prefix Diagram

File Access

File Access security groups (Figure 1-2) provide access directly on servers to unstructured data stored in shares and folders. Home drives are considered File Access but follow a separate access provisioning process found in user account management documentation.

NOTE Folder labels are defined as follows:

- Volume/Share Name — This is the folder name in the Distributed File System (DFS) path where the link is made to the share on the storage device. The folder icon appears as a *shortcut icon*, which denotes this relationship.
- Parent Folder — This is the name of the folder immediately above the access folder in the file tree.
- Access Folder — This is the folder where the group will be applied so that the user can obtain access in the file tree.

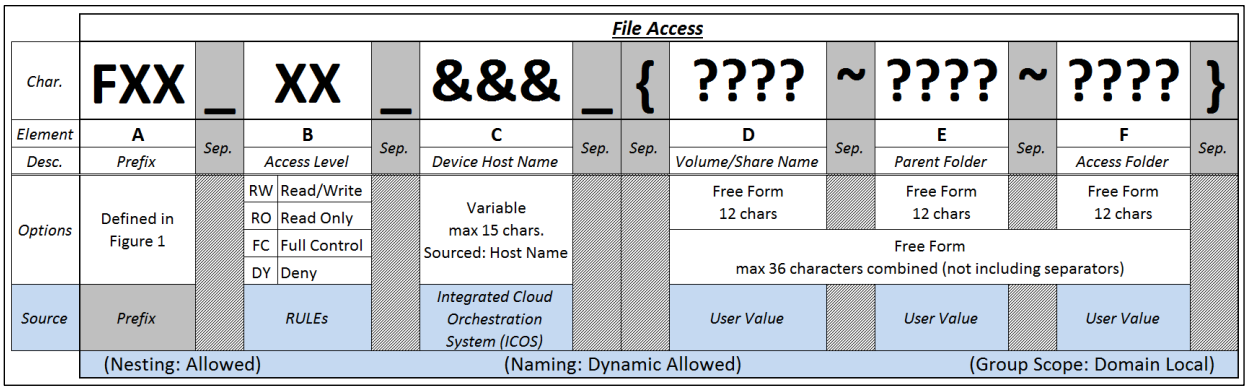


Figure 1-2 File Access Diagram

Printer Access

Printer Access security groups (Figure 1-3) are used for assigning network printer access. They are used to apply the network printer Group Policy Objects (GPOs) and permit users to submit print jobs.

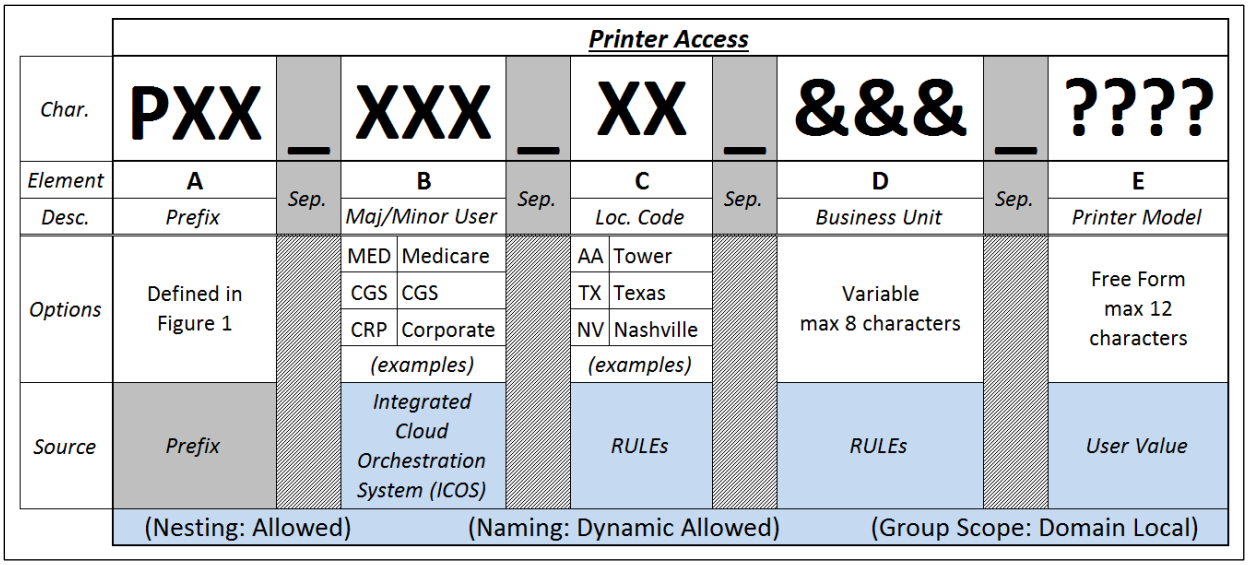


Figure 1-3 Printer Access Diagram

Application Access

Application Access security groups (Figure 1-4) are used for assigning access to network applications.

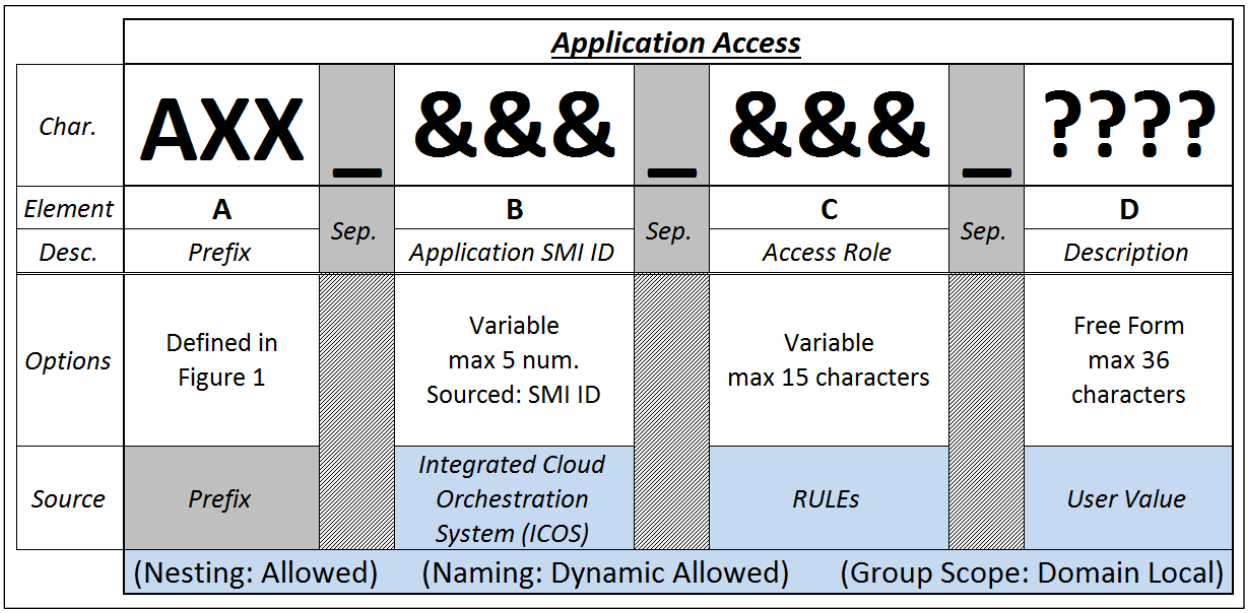


Figure 1-4 Application Access Diagram (AD)

Azure Active Directory

Azure Active Directory cannot use group attributes to denote Administrative, Restricted and Unrestricted groups. The following diagram (Figure 1-5) represents how they are identified in the group name.

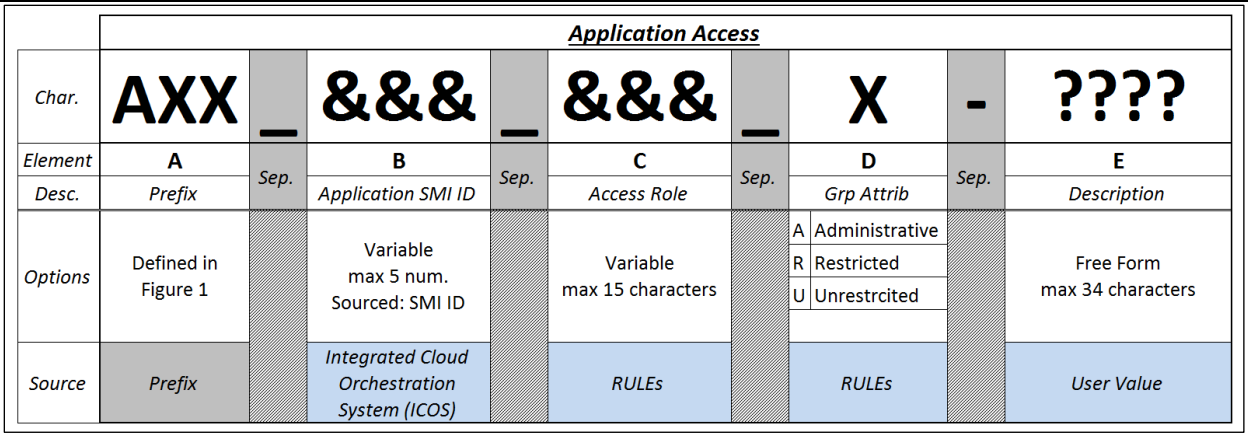
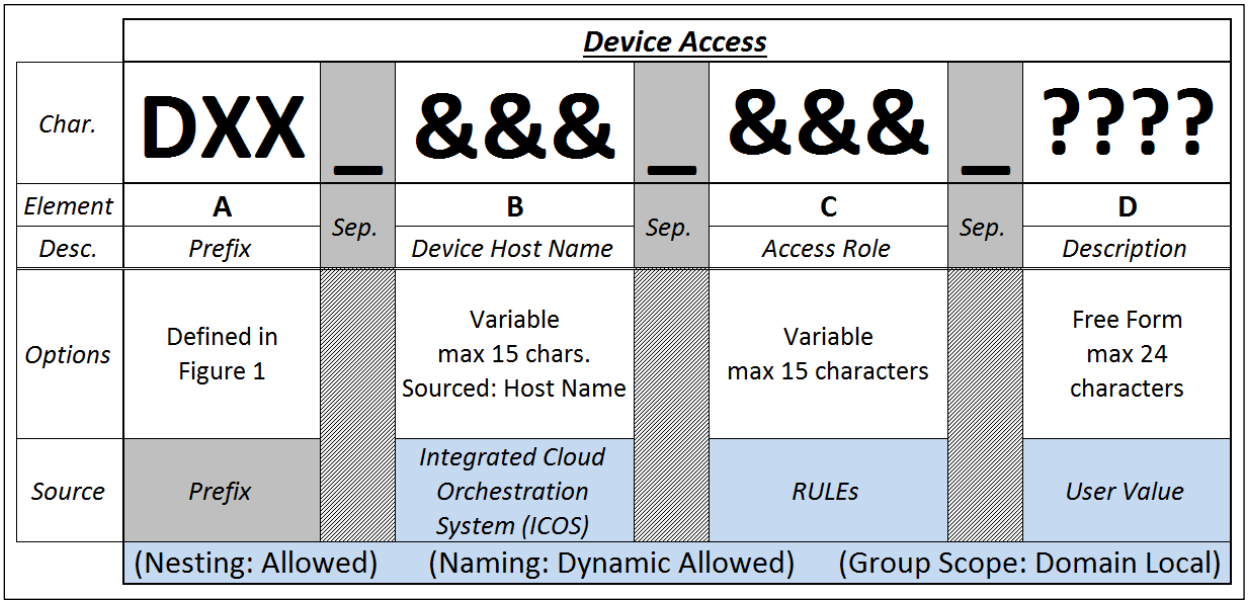


Figure 1-5 Application Access Diagram (Azure)

Device Access

Device Access security groups (Figure 1-6) are used for assigning access to devices.

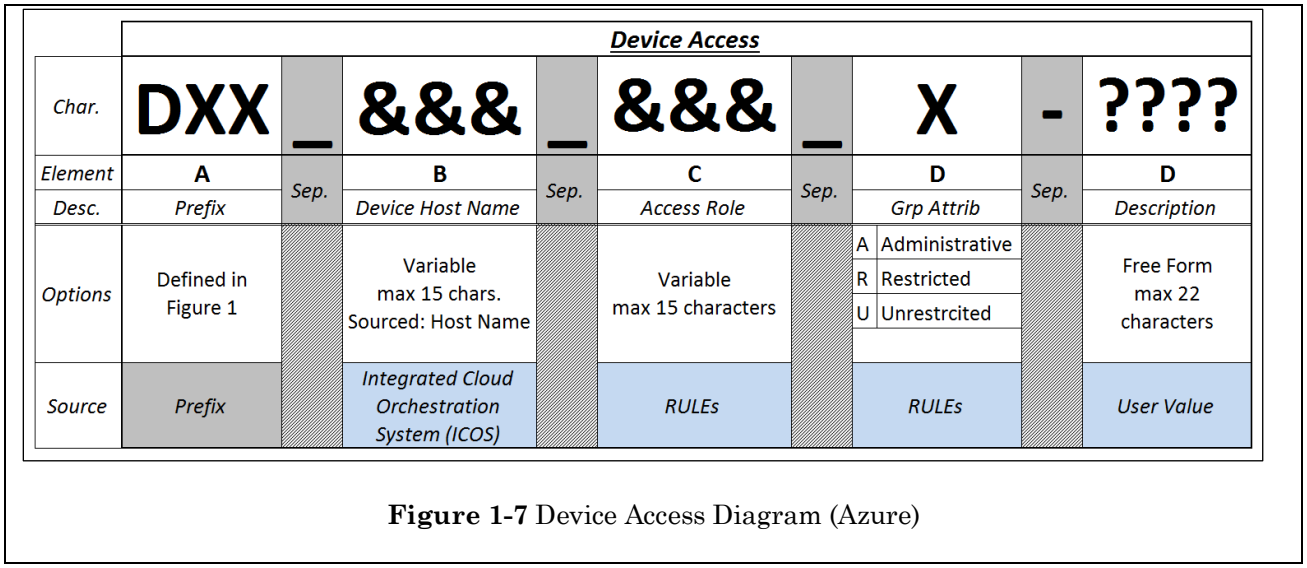


	Device Access						
Char.	DXX	_	&&&	_	&&&	_	????
Element	A	*Sep.*	B	*Sep.*	C	*Sep.*	D
Desc.	*Prefix*		*Device Host Name*		*Access Role*		*Description*
Options	Defined in Figure 1		Variable max 15 chars. Sourced: Host Name		Variable max 15 characters		Free Form max 24 characters
Source	*Prefix*		*Integrated Cloud Orchestration System (ICOS)*		*RULEs*		*User Value*
	(Nesting: Allowed)		(Naming: Dynamic Allowed)		(Group Scope: Domain Local)		

Figure 1-6 Device Access Diagram (AD)

Azure Active Directory

Azure Active Directory cannot use group attributes to denote Administrative, Restricted and Unrestricted groups. The following diagram (Figure 1-7) represents how they are identified in the group name.



	Device Access								
Char.	DXX	_	&&&	_	&&&	_	X	-	????
Element	A	*Sep.*	B	*Sep.*	C	*Sep.*	D	*Sep.*	D
Desc.	*Prefix*		*Device Host Name*		*Access Role*		*Grp Attrib*		*Description*
Options	Defined in Figure 1		Variable max 15 chars. Sourced: Host Name		Variable max 15 characters		A Administrative R Restricted U Unrestrcited		Free Form max 22 characters
Source	*Prefix*		*Integrated Cloud Orchestration System (ICOS)*		*RULEs*		*RULEs*		*User Value*

Figure 1-7 Device Access Diagram (Azure)

Delivery

Delivery security groups (Figure 1-8) are used for the delivery of network resources (application installs, Citrix published applications, GPOs, login scripts, drive mappings, etc.) to a user.

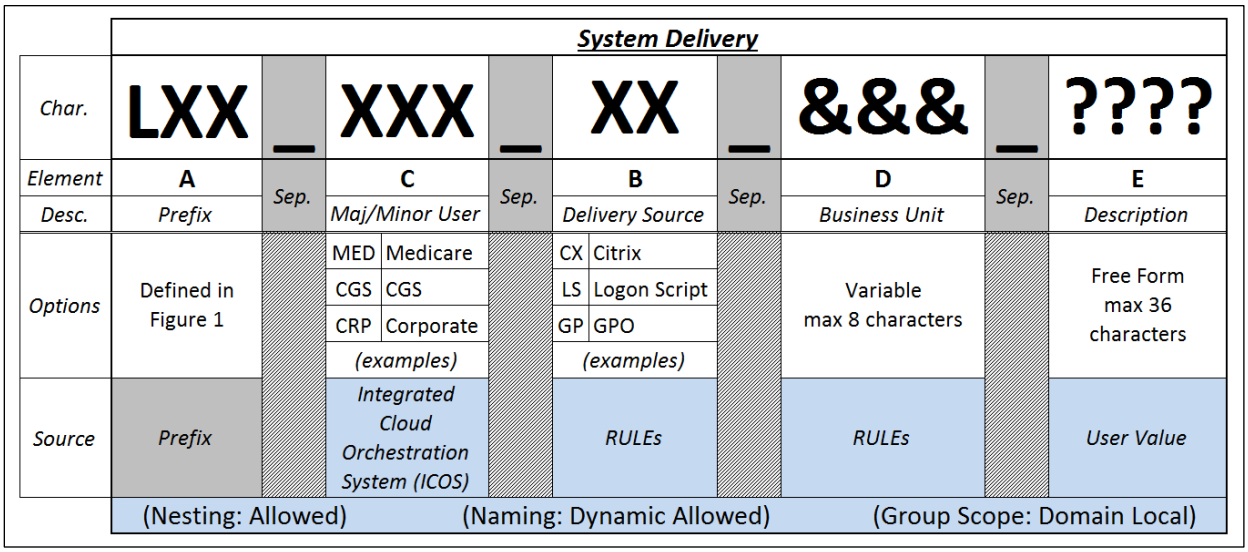


Figure 1-8 Delivery Diagram (AD)

Azure Active Directory

Azure Active Directory cannot use group attributes to denote Administrative, Restricted and Unrestricted groups. The following diagram (Figure 1-9) represents how they are identified in the group name.

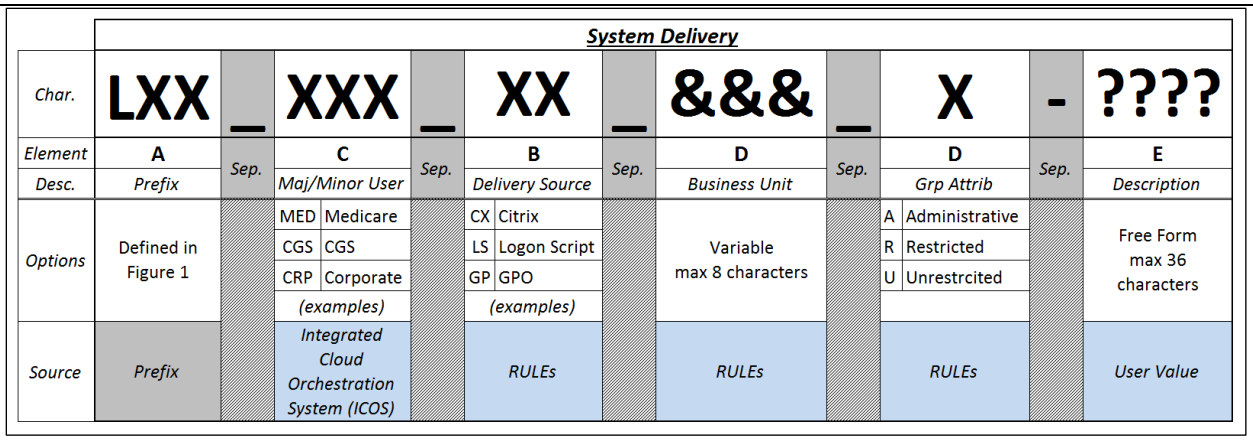


Figure 1-9 Delivery Diagram (Azure)

Unix Access

UNIX Access security groups (Figure 1-10) are used exclusively for granting access to UNIX-based systems. These groups are *UNIX Enabled* via third-party products to support UNIX access controls.

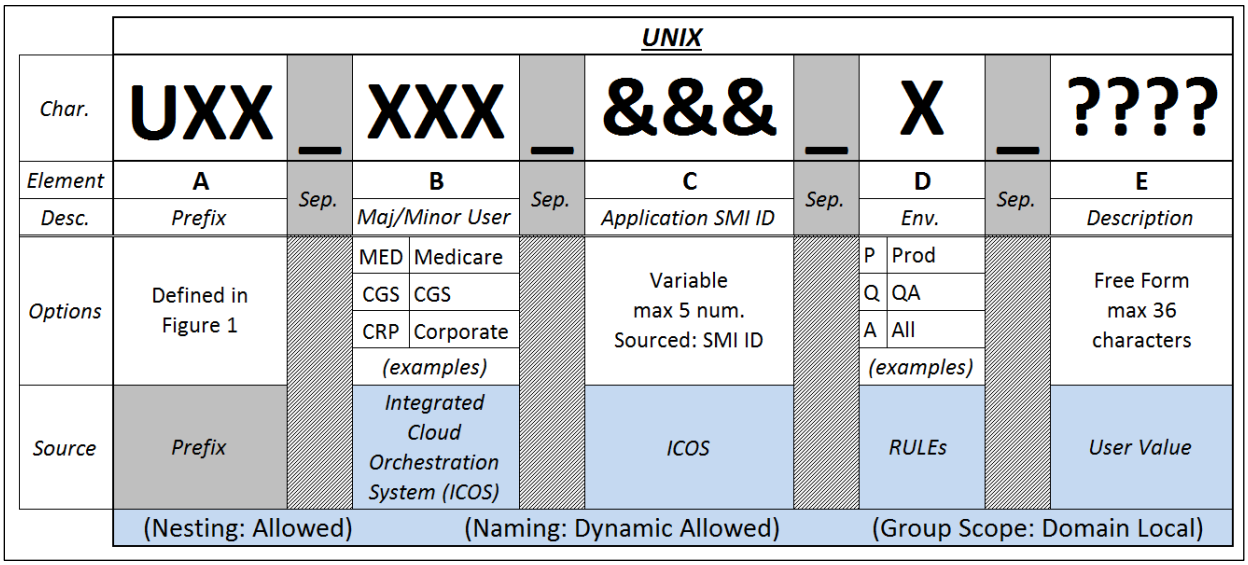


Figure 1-10 UNIX Access Diagram

Group Placement

Active Directory

Groups created using the new standards should be placed in specific Organizational Units (OUs) within Active Directory. This is to both distinguish them from legacy groups and facilitate control over which teams or persons have access to create and modify newly created groups going forward. Restriction of access to manage these groups is required to maintain the standard.

All security groups using the new standard will be placed into or below the following OU:

OU=Groups,OU=Enterprise,DC=Domain Root,DC=Domain Suffix

1.4.4 Cloud Identity and Access Management Standards

1.4.4.1 Cloud Identity Provider

A Cloud Identity Provider (IdP) is a federation partner that vouches for the identity of Business to Employee (B2E) access to cloud services. The B2E access refers to identifying, authorizing and granting access to cloud services for employees. The Cloud IdP authenticates the B2E access and provides an authentication token (information that verifies the authenticity of the user) to the service provider.

BlueCross utilizes Microsoft Azure Active Directory (AAD) as the Cloud IdP for B2E. AAD is an enterprise identity service that provides single sign-on (SSO), multi-factor authentication (MFA), and conditional access policies to secure and manage access to cloud services through B2E access.

B2E access to approved third-party cloud services and applications that store and process company data will be accomplished via SSO and AAD.

SSO provides the capability to authenticate once through a single IdP and be subsequently and automatically authenticated when accessing authorized target systems. Using SSO provides a single audit trail, passthrough of password management policies and a mechanism to enforce login rules via conditional access policies.

1.4.4.2 Conditional Access Policies

Conditional Access Policies are rules that use contextual information to apply the defined level of security to a login attempt. They are used to apply access controls to keep our organization secure. Conditional Access Policies at their simplest are if-then statements — if a user wants to access a resource, then they must complete or adhere to an expected action. When SSO via AAD is configured, conditional access policies are applied. In cases where SSO via AAD is not used, these standards are expected to be applied in an alternative manner.

The Conditional Access Policies are triggered based on user or group membership, IP address/geo location, device type, application, or risk detection. The following Conditional Access Policies are required, at a minimum:

- When authenticating as a privileged user, require MFA.
- When authenticating off network, require MFA.
- When authenticating off network, restrict access from unauthorized geographic locations.
- Block authentication via basic authentication for all users.
- Apply risk-based anomaly detection policies.

1.4.4.3 Azure Active Directory Connect

AAD Connect is an on-premises Microsoft application that's designed to allow the organization to sync existing employee accounts in Active Directory to AAD. This synchronization allows a common identity to facilitate licensing and usage of integrated cloud services, such as Microsoft 365, and minimize overhead for managing separate identities.

AAD Connect synchronizes users and groups that are flagged along with certain attributes such as name, email and password. Each user's password is never stored in AAD, and the synchronization only includes a hash, of the hash, of the user's password via a process called Password Hash Synchronization (PHS).

On-premises system administrator accounts are not authorized for synchronization to Azure Active Directory. On-premises service accounts are not authorized for synchronization to Azure Active Directory.

1.4.4.4 Use of Service Accounts in the Cloud

Service accounts are a special type of account that is intended to represent a non-human entity such as an application, application programming interface (API), or other service. These types of accounts are not authorized for use in the cloud because they do not force modern authentication, or multi-factor authentication and whose actions cannot be tied to a unique individual.

Alternatives to service accounts should be used, such as managed identity and service principal accounts. These types of accounts allow automated management of secrets and credentials used to secure communication between different services ensuring that the secret is never exposed.

To leverage service accounts in AAD, a service principal or managed identity must be used.

In cases where user-based service accounts are required, such as when service principles are not supported, an exception must be processed by sending an email to GOVERN.EXCEPTION.REQ.

1.4.4.5 Cloud Shared Responsibility Model

The section *Technical Infrastructure Architecture - Cloud Computing Definitions* in the Systems Architecture Book defines three service models for the cloud — **Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)**. When leveraging each service model, different constituents are responsible for implementing and managing different parts of the stack. This is commonly referred to as the shared responsibility model. Based on the three service models above, the cloud shared responsibility model is visualized as shown in the table below (Table 1-6). The blue shading represents cloud customers (e.g., BlueCross). The orange shading represents Cloud Provider (e.g., AWS, Azure, etc.). The purple shading represents the BlueCross Data Center.

Cloud Shared Responsibility Model

Type of Support	On Premises	IaaS	PaaS	SaaS
Compute, Network & Storage				
Hardware/ Hypervisor				
Operating System				
Middleware				
Data Access				
Applications and Data				

Table 1-6 Cloud Shared Responsibility Model

1.4.5 Data Security Standards

All requests for access to resources secured on the Host and Non-Host environments must be submitted to Data Security Administration via secured standard forms with all applicable sections completed.

Access to resources may be revoked/deleted/disabled at any time at the discretion of a Data Security Manager based upon concerns regarding security violations. When resource access is revoked/deleted/disabled, a Data Security Manager will contact the system user's management chain regarding the issues or concerns.

Data ownership by the customer area must be established during the Discovery and Delivery Strategy Phase when conducting the requirements review and communicated to Data Security Administration. This will provide the necessary points of contact for the coordination of access and security control reviews.

The data owner is responsible for specifying whether the file is sensitive, and which User IDs should be allowed access and to what level of access (e.g., read only).

The following accounts must be reviewed every 90 days:

- All accounts with access to Medicare lines of business (e.g., Palmetto GBA, CDS, CGS, etc.)
- Medicare Support accounts (For details, refer to the section *Medicare Support Definition* below.)
- All PGBA accounts

1.4.6 Applications/Software System Security Control Standards

All system or application paths will be configured to verify the UserID and password of the person requesting access.

All Enterprise software/applications must have the access control interface implemented before the product is in production status to ensure the processing environment is protected from unauthorized user access.

The Network and Enterprise Server systems for all Medicare environments are configured to provide certain information upon successful logon. Users who sign on to Time Sharing Option (TSO), CICS and Windows will receive the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

Applications and subsystems with mechanisms that require the use of an ID and password combination will use tightly controlled, strictly limited access libraries and scripts to store the ID and password pair.

1.4.7 Security below the Transaction Level

When an application or system requires security below the transaction level, the security system employed needs to adhere to the security and audit criteria stated above. The administrators of the transaction level security tables and files must ensure that the tables are modified when an employee transfers or terminates. For guidance on how to approach this issue, refer to *Security Management* > *Application Security* > *RACF Security Coding Procedures* > *Application Level Security Tables*.

1.4.8 External Security Directive

Where appropriate, BlueCross BlueShield of South Carolina will establish, deploy, and maintain application systems and application support systems developed for use within the corporate enclaves in alignment with Department of Defense (DoD) Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) guidance. In cases where STIG guidance isn't available or appropriate, other guidance may be used.

The corporate device matrix will be reviewed by Security, Risk and Compliance Assurance (SRCA) monthly to determine what technologies need baselines established.

1.4.8.1 Information Assurance-Enabled Products

All Information Assurance (IA)-enabled products procured or designed as a solution for the PGBA or Medicare enclaves must meet the Evaluated Assurance Level (EAL) specified by one or more of the standards listed below:

- Committee on National Security Systems CNSSP-11 ("National Policy Governing the Acquisition of Information Assurance [IA] and IA-Enabled Information Technology Products")
- DoD Risk Management Framework (NIST)
- Centers for Medicare & Medicaid Services (CMS) Minimum Security Requirements (CMSRs) of the enclave the product will support

An IA-enabled product is a product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control or non-repudiation of data), correct known vulnerabilities, and/or provide a layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, intrusion detection devices, security-enabled Web browsers, screening routers, trusted operating systems and security-enabled messaging systems.

1.4.8.2 Documentation for External Security Controls

Some business contracts have requirements to maintain compliance with external security controls, such as National Institute of Standards and Technology (NIST) computer security publications or CMSRs. As such, it is necessary to identify all policy and procedure documentation that relate to these security controls.

The Security, Risk and Compliance Assurance (SRCA) system serves as the Enterprise repository for documented procedures intended to support these controls. The inventory of procedures, at a minimum, includes the business process, business process owner and participants, and associated documentation that show the procedure's support of security controls. The document owner is responsible for ensuring that their documentation is contained in the SRCA system.

Content included in the ISSM does not need to be uploaded to the SRCA system. Instead, a reference to the applicable section of the ISSM should be entered there. In addition, areas that have document control procedures in place to support ISO 9001:2015 (Quality Management Systems — Requirements) registration do not need to include their controlled documents in the SRCA system. However, the SRCA system does need to index the document names to the appropriate control objectives so that they can be identified.

1.4.9 Application Security Evaluation

Prior to the acquisition and use of externally developed software or IT service, an external security assessment is required. This external security assessment will evaluate and assess the security posture of the software or IT service to determine what are the security risks if it is utilized within the environment in question.

This standard applies to all externally developed software and/or externally provided IT services within the environments supported by the I/S Division and the environments supported by the Companion Life Subsidiaries.

1.4.10 User Session Configuration and Termination

1.4.10.1 Personal Computers

All Personal Computers must be deployed with a screen saver password invoked after 15 minutes of idle time has elapsed. All Companion Life subsidiary Personal Computers must be deployed with a screen saver password invoked after 30 minutes of idle time has elapsed.

1.4.10.2 TSO Sessions

The wait time before an idle TSO session is logged off is 15 minutes via system exit IEFUTL — time limit exit.

1.4.10.3 CICS Sessions

The CICS timeout value must be set to 30 minutes on all Medicare CICS RACF User IDs.

1.4.10.4 TPX Sessions

The Terminal Productivity Executive (TPX) session manager must be configured with a password re-verification window that displays after 30 minutes of idle time has elapsed. The session must automatically terminate after 360 minutes (six hours) of idle time has elapsed.

1.4.10.5 Concurrent Connections

The number of Active Directory, CICS and TSO concurrent connections or sessions must be limited and enforced to a number required to perform job duties.

1.4.10.6 TSO Concurrent Sessions

By default, TSO limits the number of concurrent connections to one per User ID.

1.4.10.7 CICS Concurrent Sessions

The CICS concurrent connections must be set to four on all Medicare CICS RACF User IDs. Any request for more than four concurrent sessions must be approved by the appropriate VP/AVP and System Security Officer (SSO) prior to being granted.

1.4.10.8 Active Directory

The number of Active Directory concurrent connections must be set to one for all Medicare users.

1.5 Configuration and Vulnerability Management

The goal of the configuration and vulnerability management programs is to reduce the length of time a weakness is exposed. Each area responsible for maintenance and remediation should review vendor advisory notices, alerts, updates, Information Assurance Vulnerability Management (IAVM) alerts, and the various vulnerability and configuration reports as appropriate for the tools and technologies.

Nightly updates are applied to the vulnerability scan tools to ensure that we are current with the latest vulnerability checks. Self-assessments based on the vulnerability and configuration scans determine patching And configuration needs of the organization. The severity of the risk associated with a vulnerability and configuration item determines the time frame for implementing a patch.

While the SLAs noted in the sections below are the enforced standards for their respective compliance objectives, external factors such as an identified vulnerability being actively exploited in other companies may require a faster SLA be enforced on a case-by-case basis.

1.5.1 Patch Implementation/Vulnerability Remediation Schedule

Patching and vulnerability remediation are performed on intervals and at times prescribed by the compliance objectives of the business owners.

1.5.1.1 Corporate and Commercial Patching Overview

Patching for Corporate and Commercial servers follows this schedule.

Remediation for all platforms is based on weekly scans. Vulnerability findings indicated in these scans that require patches for remediation are scheduled based on risk priority (Critical, High, Medium, and Low). See the table below (Table 1-7) for scheduling details.

Corporate and Commercial Patch Maintenance and Remediation

Process	SLA
Patch Maintenance	Scheduled within SLA
Vulnerability Remediation	Critical — within 30 days High — within 30 days Medium — within 90 days Low — within 180 days
Notes: 1. Exceptions to the listed cycles are managed through a VP-approved emergency Request For Change (RFC). 2. Vulnerabilities rated as “Informational” are not applied.	

Table 1-7 Corporate and Commercial Patch Maintenance and Remediation

1.5.1.2 PGBA Patching Overview

Vulnerability remediation for in-scope platforms is based on the PGBA compliance requirements.

The remediation schedule for all platforms is based on the severity or associated risk of the vulnerabilities detected during the weekly scans. The associated risk or severity levels are Critical, High, Medium, and Low. See the table below (Table 1-8) for scheduling details.

PGBA Patch Maintenance and Remediation

Process	SLA
Patch Maintenance	Scheduled within SLA
Vulnerability Remediation SI-2 (See Note 2.)	Critical — Within 30 days High— Within 30 days Medium and Low — Within 90 days
Notes: 1. Exceptions to the listed cycles are managed through a VP-approved emergency RFC. 2. Vulnerability Remediation — Items that are not remediated in accordance with the standard are tracked with a documented MSR Plan of Action and Milestones (POAM) extension through the PGBA System Security Office. 3. Compliance Remediation — Remediation schedules are derived through output from the vulnerability remediation scan process (RA-5). RA-5 control is included to be compliant with PGBA requirements.	

Table 1-8 PGBA Patch Maintenance and Remediation

1.5.1.3 Medicare Patching Overview

Remediation for all platforms is based on weekly scans. Vulnerability findings indicated in these scans that require patches for remediation are scheduled based on risk priority (High, Medium and Low). See the table below (Table 1-9) for scheduling details.

Medicare Patch Maintenance and Remediation

Process	SLA
Patch Maintenance	Scheduled within SLA
Vulnerability Remediation	Critical —15 calendar days All others — 30 calendar days
Notes: 1. Exceptions to the listed cycles are managed through a VP-approved emergency RFC. 2. Vulnerabilities rated as “Informational” are not applied.	

Table 1-9 Medicare Patch Maintenance and Remediation

1.5.1.4 Medicaid Patching Overview

Patches are released, as applicable, by the vendor, alerts/advisory alerts, updates or IAVM. These communications are to address software bugs or feature enhancements or both. Such patches are reviewed and submitted to the Technology Owner for final approval. The patch must be installed within the applicable risk SLA, per the finding severity.

Patching for Medicaid Disaster & Recovery servers follows this schedule.

Remediation for all platforms noted with the environment is based on daily scans. Vulnerability findings indicated in these scans that require patches for remediation are scheduled based on risk priority (Critical, High, Medium, and Low). See the table below (Table 1-10) for scheduling details.

Medicaid Patch Maintenance and Remediation

Process	SLA
Patch Maintenance	Scheduled within SLA
Vulnerability Remediation	Critical — within seven (7) calendar days High — within seven (7) calendar days Medium — within 15 calendar days Low — within 30 calendar days
Notes: 1. Exceptions to the listed cycles are managed through a VP-approved emergency RFC. 2. Install updates of software or firmware or both on production equipment found unable to meet the required SLAs. The installation of these updates must be covered with the appropriate Risk Documentation and must be completed prior to the associated Risk SLA deadline. All Risk Documentation must be approved via CDS SSO Office.	

Table 1-10 Medicaid Patch Maintenance and Remediation

1.5.2 Configuration Remediation Schedule

Remediation is performed on intervals and at times prescribed by the compliance objectives of the business owners.

1.5.2.1 Corporate and Commercial Remediation Overview

CM Remediation for Corporate and Commercial devices follows this schedule.

Remediation for all platforms is based on weekly scan assessments and semiannual manual assessments. Configuration Management findings indicated in these assessments that require remediation are scheduled based on risk priority (High, Medium, and Low). See the table below (Table 1-11) for scheduling details.

Corporate and Commercial Configuration Remediation

Process	SLA
Compliance Baseline CM	High — within 90 days Medium — within 90 days Low — within 90 days

Table 1-11 Corporate and Commercial Configuration Remediation

1.5.2.2 PGBA Remediation Overview

CM-06 Remediation for in-scope platforms is based on the PGBA compliance requirements.

The remediation schedule for all platforms is based on the severity or associated risk of the vulnerabilities detected during the weekly scans. The associated risk or severity levels are High, Medium, Low, CAT I, CAT II, and CAT III. See the table below (Table 1-12) for scheduling details.

PGBA Configuration Remediation

Process	SLA
Compliance Baseline CM-06	High or CAT I — within 90 days Medium and Low — within 90 days CAT II and CAT III — within 90 days
Notes: 1. Exceptions to the listed cycles are managed through a VP-approved emergency RFC. 2. Compliance Remediation — Remediation schedules are derived through output from the compliance baseline scan process (CM-06). CM-06 control is included to be compliant with PGBA requirements.	

Table 1-12 PGBA Configuration Remediation

1.5.2.3 Medicare Remediation Overview

CM-06 Remediation for all platforms is based on weekly scans. Vulnerability findings indicated in these scans that require patches for remediation are scheduled based on risk priority (High, Medium, and Low). See the table below (Table 1-13) for scheduling details.

Medicare Configuration Remediation

Process	SLA
Compliance Baseline CM-06	High — within 30 days

Medicare Configuration Remediation

Process	SLA
	Medium — within 30 days Low — within 30 days
Notes: 1. Exceptions to the listed cycles are managed through a VP-approved emergency RFC.	

Table 1-13 Medicare Configuration Remediation

1.6 Threat Management

1.6.1 Information Security Vulnerability Management Process

The Information Security Vulnerability Management Process identifies, documents, and remediates flaws or weaknesses in information systems that could lead to the unauthorized exposure of information. The goal of the Information Security Vulnerability Management Process is to reduce the risk of system compromise to an acceptable level by reducing the avenues by which a system can be exploited.

Removing system weakness through a configuration change or an application of corrective patches is ideal. However, when immediate corrective actions cannot be made, the application of compensating security controls may reduce the risk of a system flaw being exploited. When the risk of a system compromise is sufficiently reduced using corrective actions or compensating controls, residual risk is appropriately reviewed and approval of acceptance is given.

The Information Vulnerability Management Process also seeks to reduce the length of time that a weakness is exposed. If a patch is available that corrects a vulnerability, processes should implement the fix within Service Level Agreement (SLA) requirements, addressing vulnerabilities according to the severity of risk they expose. Likewise, if a configuration change corrects a weakness, it should also be made in a timely manner and within SLA requirements. When situations occur where a vulnerability cannot be corrected according to an SLA or when remediation is not appropriate, risk and exception documentation is created. Risk and exception documentation review and approval are obtained according to Line of Business (LOB) requirements.

The following steps in the Information Security Vulnerability Management Process are described in detail below:

- Identification
- Evaluation
- Response
- Validation
- Closure

1.6.1.1 Identification

Vulnerabilities or weaknesses can be identified at any time. Some common trigger events are:

- Audits — Audits sample a representation of systems and processes and may detect situations where corrective action is needed. When sampled systems are identified as having vulnerabilities, efforts should be made to review like systems that were not part of the audit for the same vulnerability.
- Proactive scans — Network scans of attached devices regularly detect vulnerabilities and serve as confirmation by absence that previous vulnerabilities have been corrected.
- Self-assessments — The use of periodic checklists or other specific self-assessments of systems can identify weaknesses.

- Vendor notifications — Vendors report flaws to national databases and often to individual companies depending on service or support agreements.
- DMM Compliance Acceptance Review — Evaluation of any newly deployed or modified infrastructure to ensure it meets security and audit requirements.

1.6.1.2 Evaluation

An identified vulnerability is evaluated to assure validity. If valid and if the vulnerability is related to a system's configuration, firmware, or software flaw, a review of any available fix steps or vendor patch is made. Consideration is given to whether the flaw can be remediated within the required Service Level Agreement (SLA), and if other compensating actions can be performed to reduce the exposure of the vulnerability.

The evaluation will be conducted by the support area responsible for the impacted process or component. The evaluation process is expected to occur quickly to meet the SLA requirements to remediate vulnerabilities.

1.6.1.3 Response

If a system configuration, software, or hardware flaw can be directly remediated, the appropriate system changes are applied. If the vulnerability cannot be fully remediated within the related SLA, one of the following risk or exception documents must be completed and entered into the central repository for risk and exception documentation. The responsible support area will create the risk and exception documentation.

- Mitigation Strategy Report (MSR)
- Policy/Procedure Memo
- Business Risk Justification (BRJ)
- False Positive Document
- Plan of Action and Milestones (POA&M)

Table 1-14, "Line of Business Documents" (on the next page), shows which documents are used within each LOB.

Line of Business Documents

Risk or Exception Document Type	PGBA	Medicare	Commercial/ Corporate
Mitigation Strategy Report (MSR)	X		
Policy/Procedure Memo	X	X	X
Business Risk Justification (BRJ)		X	X
False Positive Document	X	X	X
Plan of Action and Milestones (POA&M)		X	X

Table 1-14 Line of Business Documents

NOTE The MedAdvantage contracts are under the Commercial LOB and not Medicare.

Mitigation Strategy Report (MSR)

A Mitigation Strategy Report (MSR) is only applicable to the PGBA LOB and is required for the following circumstances:

- A vulnerability within the PGBA enclave cannot be resolved using the accepted recommendation as specified by the supporting documentation and requirements referenced within Department of Defense (DoD) Security Technical Implementation Guides (STIG), internal vulnerability matrices or other PGBA contractual requirements, but the vulnerability is mitigated using an alternate solution.
- A vulnerability cannot be remediated within the set remediation SLA time frame, and an alternate time frame is documented.

Policy/Procedure Memo

A Policy/Procedure Memo is used to address vulnerabilities in situations where a perceived vulnerability is actually acceptable given the circumstances of use. A Policy/Procedure Memo is generally used to remediate configuration related vulnerabilities where the use of a configuration setting that otherwise is considered a vulnerability is deemed to be acceptable because of the context of its use and the fact that it is known and has been documented. This is typically the case when it is noted in the DoD STIG that a requirement is "documentable with the IAO/ SSO [System Security Officer]," and the requirement can be met. Examples of this would be required services, accounts, account settings, password settings, etc. This document is used by all LOBs.

Business Risk Justification

A Business Risk Justification (BRJ) is an exception document used to record the acceptance of risk that remains in situations where a vulnerability is unable to be fully remediated. A BRJ contains a description of the vulnerability, statements regarding compensating controls in place to reduce risk, and a judgment of impact to the organization based on the residual risk.

A BRJ is created when a control cannot be configured according to selected guidance (e.g., DISA STIG, USGCB, CMSRs) requirements. There are two classifications for BRJs:

1. Deviations are **platform-wide** control configurations that must be set consistently across each device within a given platform to support the business mission. Configuration settings identified as Deviations will be applicable to all devices within a platform.
2. Exceptions are **system-specific** control configurations that must be set on one or more specific devices but not all devices in a given platform to support the business mission. Configuration settings identified as Exceptions must also indicate the percentage of systems the Exception impacts and the Hostnames of those systems.

A BRJ is used for Medicare and the Commercial/Corporate LOBs.

False Positive Document

False Positive documents are used to record verified situations where a scanning tool may not be able to properly differentiate between a setting that indicates a true vulnerability and one that may not be. When a false positive is suspected, the scan tool support area must be contacted so that an inquiry is made with the scan tool vendor or addressed by the scan tool support team if it is an internally developed check. If the vendor responds by changing their detection script, the vulnerability should no longer be detected. If the vendor responds that the vulnerability is being properly detected, further investigation of the detected vulnerability by the remediation area must be made regarding the circumstances of the detection. For an internally developed check, the scan tool support team will make the determination if the vulnerability is being properly detected or will work with the remediation area to further investigate the false reporting, making adjustments to the internal check as necessary. If the remediation area's stance holds that the vulnerability is being falsely detected, a False Positive document should be created for approval. Otherwise, if other remediation solutions such as a configuration change or patch are not available, a BRJ document should be submitted to document the risk acceptance.

The False Positive document is used for all LOBs.

Plan of Action and Milestones

A Plan of Action and Milestones (POA&M) identifies the steps to be taken to address a vulnerability that cannot be remediated within the given SLA. A POA&M should provide a list of associated actions and milestones with their respective scheduled implementation timeframes. Because additional reporting and response is required with the use of a POA&M, all efforts should be made to avoid use of POA&Ms by completing work efforts within SLA timeframes.

POA&Ms are used for Medicare and Commercial/Corporate LOBs.

1.6.1.4 Validation

Validation is used to assure that corrective actions have been taken. Validation can take one of two forms:

- The validation of the technical changes made to remediate the vulnerability
- The review and approval of the risk and exception documentation

If the vulnerability is remediated through technical changes, those changes are reviewed via scan results, manual review, or other steps necessary to determine that the expected result has been achieved.

If the vulnerability response is in the form of risk or exception documentation, the following risk and exception document life cycle occurs.

Risk and Exception Document Life Cycle

Each risk or exception document has a life cycle that it undergoes from its inception through final approval.

The life cycle consists of the following stages:

- Initial document drafted by the technician
    - Appropriate documentation must be included, and will vary dependent upon the document
- Management review and approval by the technician's direct management
- Compliance review by the SRCA Team
- Compliance review and final approval by the appropriate LOB System Security Officer (SSO)
    - For Medicare it is the corresponding SSO
    - For PGBA it is the Security Manager
    - For Commercial/Corporate it is the Chairman of the Corporate Security Council

Throughout the risk and exception document life cycle, any changes and approvals must be added in the Comments tab of the document. If any issues are uncovered during the life cycle, the document will be returned back to the prior step for resolution and will then continue back through the subsequent steps of the life cycle.

1.6.1.5 Closure

The closure of a vulnerability is dependent upon the type of response that was undertaken.

If the vulnerability is fully remediated through applying the necessary system changes, closure occurs when the validation step is completed.

If the vulnerability is determined to be a False Positive, addressed through a Policy/Procedure Memo, BRJ, or MSR that documents an alternate mitigating solution, the closure of the vulnerability is dependent upon the LOB to which it applies:

- For the Medicare LOBs, the vulnerability is reported closed when the draft of the risk and exception document is placed into the risk and exception documentation repository.
- For the PGBA and Commercial/Corporate LOBs, the vulnerability will not be considered closed until the documentation completes all of the various stages of the life cycle and receives the final approval by the LOB SSO.

If the vulnerability is addressed by a POA&M, or an MSR that documents a plan of action, the vulnerability remains open until the POA&M or MSR is executed and validated.

1.7 Malicious Code Protection

Immediate (as required functionality allows) installation of vendor-supplied service packs, hot fixes, security patches, and virus definitions is enforced. Vendor-supplied security patches are obtained, analyzed for security and functionality in a test bed environment, and implemented on production equipment within the allotted time, or sufficient workaround procedures are in place to protect system assets.

Network administrators ensure that malicious code software or services are enabled and operating properly on network assets, workstations, servers and containers. The virus detection software on the workstations is updated and distributed by the ePolicy Orchestrator (EPO) Management server and/or manually. For the cloud network environments, software is enabled to identify threats and potentially unauthorized and malicious activity.

These systems are configured to scan critical system files during system boot and when files are accessed. The systems will also block and quarantine malicious code and send alerts to system administrators in response to malicious code detection. All alerts are investigated to mitigate the damage caused by malicious code. Containment, eradication and recovery are very important and must be done as quickly and efficiently as possible to mitigate risk to confidentiality, integrity, and availability.

1.8 Windows Server Security

1.8.1 Commercial Windows Server Security Configuration

This standard applies to the Windows Non-Host environments for the Commercial Line of Business.

BlueCross is subject to information security requirements imposed by Federal laws such as Health Insurance Portability and Accountability Act (HIPAA), and by contracts with Federal and State agencies such as CMS and TRICARE. BlueCross has corporate policies in place to meet the requirements. To determine if there are any possible risks with the security configurations, ICT Non-Host will routinely perform scans of the systems. Information Systems will respond to these risks as described in the section *Remediation of Findings for Commercial Configuration* below.

1.8.1.1 Security Configuration Settings

Log File Maintenance and Monitoring

To facilitate the observation of information security threats and ensure forensics evidence is available when needed, ICT Non-Host will configure the systems to maintain logs which will record, at a minimum, the following events:

- Failed logon events
- Successful and failed account management events
- For Non-Host Platform, failed directory service access
- Failed attempts to access objects
- Successful changes to security configuration policy settings
- Failed attempts at privilege use
- Successful system events

ICT Non-Host will monitor the logs to observe potential breaches of information security. Any potential breaches may be reported using the Incident Management process.

Guest Accounts

Use of guest accounts is not allowed. To prevent users from logging on anonymously or accessing information without authentication, guest accounts will be secured and disabled.

Administrator Accounts

Default local system administrator accounts are secured to prevent unauthorized control of the system.

High Risk Services

Those services considered high risk because they have potential of allowing a security breach are listed in a catalog.

User Rights Assignments

Those User Rights Assignments that control advanced privileges are listed in a catalog which is routinely reviewed.

1.8.2 Security Assessment and Authorization

The following section defines how the organization shall:

- Periodically assess the security controls to determine if the controls are effective in their application.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities.
- Authorize systems operation and any associated connections.
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

1.8.2.1 Security Controls

Security is applied at both the workstation and server levels for all facilities. In order to maintain a secure and stable network environment, the ICT NH Compliance Management Enclave Definition (ICT NH CMED) group has been directed by the Senior ICT NH Management to periodically scan all network assets.

Internal Vulnerability Scanning Practices

The ICT NH CMED group conducts vulnerability scans to validate that operating systems and major applications are up-to-date on security related issues. Results are documented, and discovered deficiencies are forwarded to the appropriate group for corrective action.

ICT NH CMED utilizes security tools including, but not limited to, Nessus and AppDetective to scan the network for vulnerabilities and security holes. These security scanning tools are updated with new product patches and revisions as released by the specific vendors.

The ICT NH CMED group performs scans quarterly. To meet a customer's requirements, a Line of Business (LOB) or a subsidiary may need additional or more frequent scans. Scan results are input into a Vulnerability Matrix Report and distributed to the responsible group. Each group is required to respond with the proper corrective action.

Penetration Testing

The Cybersecurity Operations (SecOps) team uses an intrusion methodology that mimics the process used by hackers to gain access to information and systems. Due to the potential production impact and disclosure of sensitive information, SecOps is the only area authorized to conduct penetration testing of the network and its systems.

The SecOps team performs scans, tests, analyses, and attack procedures from the internet against the network. External penetration testing is performed quarterly to evaluate BlueCross' external security

posture. In addition, there is an annual internal penetration test for each LOB. Findings and assessment results are documented and vulnerabilities are correlated to the Common Vulnerabilities and Exposures (CVE) naming convention when applicable.

After the scanning process is completed, the SecOps group reviews the results and puts the data into a report format. The data is then distributed to the responsible area for remediation. Security, Risk and Compliance Assurance (SRCA) gathers updates on the status of the findings and follows up until all findings are mitigated.

1.8.2.2 Rules of Behavior

Acceptable Use and Guidelines for Application Systems

In order to establish effective expectations of Non-Host Application Support personnel regarding access to the servers on which applications reside, the following processes and procedures by which access will be granted or revoked and acceptable use/guidelines for application systems include:

- All necessary access must be documented on the Server Administrative Access Request form.
- No administrative access will be granted other than what is absolutely necessary to administer the application.
- Application Support personnel are not authorized to make changes to any Operating System settings or administrative settings on the application servers.
- ICT NH Management has the right to revoke access at any time for system-related behavior that is deemed inappropriate.

Sharing Data with Non BlueCross Entities

Sharing of data or programs is not practiced within the BlueCross Data Center. Vendors and Business Partners are required to sign an agreement to protect sensitive data. Hardware and software vendors at the BlueCross Data Center may come across sensitive data in the course of their work, but this data is not shared with them.

Collaborative Computing

Collaborative computing mechanisms are allowed provided remote activation is not enabled. Collaborative computing is defined as any interactive multimedia conferencing application that enables multiple parties to collaborate on textual and graphic documents. This includes the use of video and voice conferencing when performed using a desktop PC.

Rules of Engagement for External Penetration Testing

Auditors and/or contracted companies will conduct external penetration testing against the BlueCross network. Testing is scheduled, and ICT NH requires to be informed of the Internet Protocol (IP) address range the scans will be originating from and the times that scan will be performed.

Denial of Service exploits are not to be run against BlueCross assets.

ICT NH requests to be notified of any major vulnerability immediately so they can be addressed in a timely and appropriate manner.

1.8.3 Planning

The following section defines how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

1.8.3.1 Security Plans

Security control reviews, internal and external audits, and risk assessments are maintained and stored within the SRCA group or I/S Audit department. Periodic assessments are performed on the BlueCross Data Center to ensure that all security controls meet acceptable contractual standards and are part of the certification process.

Server Configuration Checklist

The Server Configuration Checklist contains the base items to be performed on a new server build for all platforms. The checklist also has individual tabs for specific settings, software or network needs for specialized applications. Server configuration configurations are reviewed by SIM on an annual basis (within 365 days) to assure that all of the security requirements are being met.

Security Configuration for Network Devices

This Security Configuration for Network Devices contains configuration templates to be followed when configuring a new switch, router or PIX firewall. Switch, router and PIX firewall configurations are reviewed by SIM on an annual basis (within 365 days) to assure that all of the security requirements are being met.

Internal Documentation Review

All internally generated documentation including work instructions, operational checklists, or job aids used to assist in completing Infrastructure updates should meet the following requirements:

- Each document should be reviewed and updated at least once within 365 days or as needed when significant changes have been made to the supporting systems.
- Each document should be dated and version-controlled, including reasons for the document updates. The version record must contain the following information and appear in a table like Table 1-15, “Version Record Example,” shown below:

    - Document Version number
    - Date of review or update
    - Name of reviewer
    - Description of change

Version Record Example

Ver. #	Date	Name	Description of Change

Table 1-15 Version Record Example

1.8.3.2 Portable Computing/Network Devices

Only approved portable computing and portable network devices are allowed to be connected to the BlueCross network. All portable devices including wireless have to meet the approval of the Chief Information Officer (CIO).

The SecOps team will conduct quarterly sweeps of the BlueCross network for unauthorized wireless devices or access points. If wireless devices or access points are found then the appropriate level of management is notified depending on the case for action to be taken.

USB Devices

When managing PGBA or Medicare systems, approved company-purchased Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2) certified hardware encrypted Universal Serial Bus (USB) jump drives are required. Classified, Protected Health Information (PHI), Personally Identifiable Information (PII), or Payment Card Industry (PCI) data should never be placed on USB jump drives and all approved drives must be password protected. SecOps will maintain a list of approved models.

Area management or team lead must maintain a log sheet to track the use and location of each USB drive. The drive must be sanitized upon return.

Wireless USB devices, including Wi-Fi, Bluetooth and Cellular devices, may not be connected to any PGBA system or network.

USB jump drives, small devices that contain flash memory, are considered media and are allowed. However, jump drives and drives that are designed to look like anything other than a jump drive will not be attached to BlueCross systems. Examples of these disguised jump drives include pens, watches, jewelry, etc. Since they could easily be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a location, disguised USB jump drives will be banned from locations containing sensitive data. There is a prominently displayed notice describing this ban at all BlueCross Data Centers that contain PGBA (Department of Defense [DoD]) systems and/or data. These devices will be confiscated if found.

Mobile Device Security and Sanitizing

Information Systems areas that develop and support applications presented on mobile devices may utilize these mobile devices during development, validation, and production support.

When Incidents are resolved or when Implementation Validation sign-off and the closure of all defects of mobile applications are completed, I/S will sanitize the mobile devices to remove all potential PHI, PII, and Credit Card Account Information (CCAI).

The users of these mobile devices will enable a password or an authenticated screen lock on the mobile devices. These devices will be maintained and physically secured to be available for future efforts.

1.8.3.3 Roles and Responsibilities

There are many types of system and network users. These users have been identified and their role defined in the ISSM. Refer to *Security Management > Information Security Management > Security Roles*.

To ensure that associates understand their security duties and responsibilities, ICT NH ensures that each member receives security training and requires that they sign a document indicating they understand their job's security responsibilities. ICT NH conducts audits, training, and access reviews to ensure that the segregation of duties principle is followed.

1.8.4 System and Services Acquisition

The following section defines how the organization shall:

- Allocate sufficient resources to adequately protect organizational information systems.
- Employ system development life cycle processes that incorporate I/S considerations.
- Employ software installation and usage restrictions.
- Ensure that third-party providers employ adequate security measures to protect information applications, and/or services outsourced from the organization.

1.8.4.1 System Development Life Cycle

ICT NH utilizes automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. Specific automated mechanisms are defined within each team's procedures.

1.8.4.2 Software Usage Restrictions

Information Handled

The information processed and stored within each business unit meets the definition of sensitive but unclassified data, as described in the Office of Management and Budget (OMB) Circular A-130, "Security of Federal Automated Information Resources," because it contains personal, medical, and financial data, and data protected by the Privacy Act of 1974 and the Freedom of Information Act of 1986. Personal health information is protected under HIPAA. System owners are required to determine the appropriate system security level based on the information's confidentiality, integrity, availability, and its criticality to the agency's business mission.

Overall System Security Level

The overall system security level for the information processed and stored is High. Based on the information alone, the system security level would be designated Moderate from the following information categories: information about persons and other federal agency information.

Guided Media

Concerning the use of encryption or guided media for file transmission as it pertains to the Centers for Medicare & Medicaid Services (CMS) data. Transmissions of Medicare data is not approved across the internet by CMS. The only forms of transmission of Medicare data is through a NDM connection through the CMS network (CMSNet). Validation of Secure File Transfer Protocol (SFTP) data transmission is performed across the CMSNet network as well, since Medicare has approved this form of transmission.

1.8.4.3 Interconnection and Information Sharing

The Contracts Department finalizes approvals and authorization for interconnections to all systems (including systems owned and operated by another program, agency, organization, or contractor) and controls have been established and disseminated to the owners of the interconnected systems. After interconnects are approved, the ICT NH architecture area designs and reviews the requirements to ensure the connectivity meets all security requirements.

A network of servers supports operations and data interchange. An Asynchronous Transfer Mode (ATM) Wide Area Network (WAN) supported by gateway routers provides connectivity. These servers support the flow of sensitive data between the Enterprise Server and both internal and external user terminals.

External interfaces are those connections to the Enterprise Server that allow for entry or access to the Enterprise Server located in the BlueCross Data Center in Columbia, South Carolina. Refer to each line of the business General Support System (GSS) System Security Plan (SSP) for a detailed description of the applications and the functions that each supports.

1.8.5 Technical Class

1.8.5.1 Identification and Authentication

The following section defines how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes or devices as a prerequisite to allowing access to organizational information systems.

Network Time

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP allows synchronized data and is significant in securing the integrity of information and data being logged. NTP is used as a single time source to relate event and audit logs.

Network Devices pull time from one of two NTP servers. The NTP servers pull time from the U.S. Naval Observatory. All Intel servers pull time from Domain Controllers. The Domain Controllers pull time from the NTP appliances that pull time from the U.S. Naval Observatory. All Reduced Instruction Set Computer (RISC) servers pull time from an NTP server that pulls its time from the U.S. Naval Observatory.

Identity Management

User Authentication

Authentication is used to:

- Restrict access to critical systems/business processes and highly sensitive data.
- Control remote access to networks.
- Grant access to the functions of critical network devices.

Procedures for the above are documented.

Generic, Group, System or Domain Authentication

The domain administrator password, the UNIX root passwords and Structured Query Language (SQL) local admin account (SA) passwords will be kept secure at all times and used only in emergency situations. The secure passwords will be sealed in three envelopes and the director of ICT NH, the director of Server/Network Deployment, and the manager of the Security Information Management team will each store one of these envelopes in a secure location. The sealed envelope containing the passwords will remain sealed at all times unless ICT NH has determined a need to use the passwords due to an emergency.

Disabling and/or changing default passwords, log-ins, and generic group/accounts and changing default security settings to more secure settings is part of enhancing the security (hardening) process when new software or systems are installed. All vendor-supplied default log-ins, passwords, and security parameters are disabled and immediately replaced or reinitialized to more secure settings.

Microsoft Windows servers install with a default administrator account that does not require a password. This account is changed along with the verification that the default "guest" account is disabled upon installation. In the AIX/UNIX/CISCO environment, the accounts named "Administrator," "Root," and "Guest" are either changed or disabled as appropriate during installation and configuration.

Password Management

The use of password and access control measures are in place to identify who accessed protected information, limit that access to persons with a need-to-know, and prohibit the use of access scripts containing embedded passwords.

Password Policy

BlueCross' password policy is listed below:

1. By default, password files in Windows and UNIX environments are encrypted at the server level for security.
2. Restrict server console access to developers who have completed an Administrative Access Request form with management approval authorizing the account.
3. Server is audited to provide a trail of configuration changes made to the server. Because the account is shared, identification of the user making changes can then be determined by examining DSView's logs (KVM solution).

1.8.6 Operational Class

1.8.6.1 Physical and Environmental Protection

The following section defines how the organization shall:

- Limit physical access to systems, equipment, and the respective operating environments to authorized individuals.
- Protect the physical facilities and support infrastructure.
- Provide supporting utilities.
- Protect systems against environmental hazards.
- Provide appropriate environmental controls in facilities.

Physical Access

Unless otherwise noted, all facilities use a C*CURE 800® access control system installed on all doors to the exterior and on selected interior doors. Access to an area is gained by using a 37-bit proximity card that is encoded to allow access to secure areas and limit the amount of time access is granted based on the employee's job function. Some areas within the building require the card to be used for exiting and entry. Terminated employees surrender their badges to the Facility Security Officer, who then deletes the access code from the system. Extra badges and the master password list are only available through the Facility Security Officer.

As per BlueCross Corporate Policy 65287, "Corporate Access Control," each person that is admitted into BlueCross facilities must have either a photograph identification (ID) card or a temporary ID card visibly displayed at all times.

All visitors must sign in at the main entrance, where they are given a numbered and a brightly colored "Visitor" badge, that must be worn at all times and returned upon leaving the building. All visitors are required to record their name, company or entity, purpose of visit, point of contact, time in, and time out. While on the premises, visitors are accompanied by an employee at all times. Time sensitive strips are used on the visitor badges to indicate their validity. Employees and contractors leaving or entering a facility are subject to a random inspection of any packages in their possession.

Physical Protection

Many physical security controls are common to all facilities. Contract security forces provide facility monitoring for access and coordinate emergency response, as necessary, for fire, police, or medical calls. Fire call boxes and fire extinguishers are clearly marked and strategically located throughout all buildings. Maintenance personnel periodically validates compliance with regulations established by the Occupational Safety and Health Administration (OSHA).

Environmental Hazards

Fire extinguishers are clearly marked strategically located throughout all buildings. Maintenance personnel periodically test fire extinguishers in compliance with regulations established by the OSHA.

The BlueCross Data Center is protected by a Factory Mutual (FM)-200 fire suppression system, which has sensors designed to detect the presence of smoke and the build-up of heat. The system includes a

locator panel visible throughout the BlueCross Data Center, which indicates the location of an unsafe condition. If a standard fire extinguisher cannot contain a fire, the FM-200 System will be activated. The robotic tape silos have self-contained extinguishing systems. Short of a major conflagration, there is no need for anyone other than authorized personnel to attend to a fire-related emergency in the computer room. Since these suppression systems will not damage equipment or documents and leave no toxic fumes, vendor access after a fire is minimized.

A parallel Exide Electronics Uninterruptible Power Supply (UPS) System protects all computer equipment, security system, surveillance access cameras, and emergency lighting from power surges and dips. Should a power interruption occur, the UPS system contains sufficient battery power to enable operators to engage in a controlled shutdown, thereby avoiding damage to equipment and data. In the event of a prolonged failure, the security system, the surveillance/access cameras, and the emergency lighting will continue to draw power from UPS batteries.

Even though the UPS system will sustain power to the BlueCross Data Center long enough to affect a "soft" shutdown, substantial losses can occur as the result of a sustained power outage. To prevent such losses due to extended outages, BlueCross installed a diesel generator backup system. The system includes two 750 KW Cummins Units, providing continuous standby duty generators, transfer switches, a 3,000 gallon diesel fuel tank, and inputs for UPS compatibility.

1.8.6.2 Contingency Planning

The following section defines how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-Disaster Recovery to ensure the availability of critical information resources and continuity of operations in emergencies.

Disaster Response

In the event of a disaster, there are business recovery procedures in place for critical facilities and operations in the form of Disaster Recovery Plans and Business Continuity Plans. Disaster Recovery and Business Continuity exercises take place annually. Lessons Learned are recorded from these exercises and are used as part of the training of the Disaster Recovery teams. Documentation of Disaster Recovery plans can be obtained from the Disaster Recovery Program Office (DRPO). Additional information on Continuity Management can be found at *Service Management > Service Delivery > IT Service Continuity Management*.

Business Continuity of Cloud Services

Cloud services necessary for the business must have a Disaster Recovery Plan, and critical cloud services should be included in Disaster Recovery Exercises. Backup and recovery operations must adhere to the RTO & RPO within the DR Plan. Refer to *Service Management > Service Delivery > IT Service Continuity Management* for more information.

Contingency Planning — Backup Operations

Backup Operations — Off-Site

When on-site storage is not available, commercial storage facilities are used that most closely meet federal standards for agency records centers. Daily backups of critical files are created, maintained, labeled (name, date, and time), and rotated to an off-site location. Library logs will be protected from

exposure to unauthorized changes or release. All deposits and withdrawals of program tapes and other storage media to/from the library are authorized and logged. Access is restricted to the tape librarian who ensures that they are released to personnel listed as having a legitimate requirement. BlueCross currently uses an off-site fireproof vault for Disaster Recovery storage. This facility is located at 4101 Percival Road in Columbia, South Carolina. Backup information is found in the Disaster Recovery Plan with detailed information contained in the ISSM. Refer to *Service Management > Service Delivery > IT Service Continuity Management > Disaster Recovery Plans.*

Daily backups of critical files are created, maintained, and rotated to an off-site location to avoid disruption if current files are lost or damaged. All tapes will be rotated on a regular schedule to an off-site storage facility. The off-site rotation schedule is as follows:

- All tapes will be sent off-site for storage Sunday through Saturday.

Only authorized personnel will be able to recall tapes early or sign for the receipt of tapes that are returned or sent off-site. All paperwork concerning delivery and pickup of tapes shall be retained for no less than one year. Users requesting a restore, for which the tapes are off-site, will be informed that the user's Cost Center will be charged the cost of returning the requested tapes.

Additional materials and resources that are stored off-site include:

- Forms and printer supplies
- System software documentation
- Applications software documentation
- Operations documentation
- Backup tape rotation documentation
- Policy and Procedures Manual

Backup Operations — On-Site

To perform backups, ICT NH uses a combination of Tivoli Storage Backup Manager (TSM) and Commvault.

TSM maintains and tracks system and user data via its database, tape pool and copy pool. The TSM standard for backups is to execute a full backup initially, and daily incremental backups thereafter. For the Medicare environment, a full TSM backup is also done weekly, and Cyclical Redundancy Checks are done to provide integrity checking. TSM backup frequency for databases is configured by Database Application (DBA) owners of the ICT DBA.

Commvault maintains and tracks user and system data via its database and storage pools. As data is written to the Commvault system in Nashville, TN, it is replicated to a secondary Commvault system at the Disaster Recovery facility. The Commvault standard for infrastructure (server) backups is to execute a full backup initially, and daily incremental backups thereafter. Weekly backups are performed by taking the last seven (7) days of incremental backups and creating a full backup sync point in the Commvault application. The standard backup retention policy of 30 days is used with Commvault.

At the request of the customer, TSM or Commvault backups can be tailored to meet customer needs and requirements.

Physical Location of Backups and Safeguards

The physical location of backups and safeguards for the ICT NH Division is the responsibility of the BlueCross Data Center. Current backup data files needed for Disaster Recovery are stored in an off-site, fireproof vault located separately from the BlueCross Data Center. Access to this vault and removal of any tapes is restricted solely to the tape librarian who ensures that backup tapes are released only to authorized personnel. Analysts, data management analysts, and the System Security Officer (SSO) follow procedures to determine the risk involved and apply the appropriate safeguards.

Alternate Processing Site

Alternate processing is covered under the BlueCross Disaster Recovery Plan in the ISSM. Refer to *Service Management > Service Delivery > IT Service Continuity Management > Disaster Recovery Plans*.

Contingency Planning

Documentation of Disaster Recovery Plans can be obtained from the DRPO.

1.8.6.3 Media Protection

The following section defines how the organization shall:

- Protect media, both paper and digital.
- Limit access to information to authorized users.
- Sanitize or destroy media before disposal or release for reuse.

Production Media Marking

All information and data processed and stored at BlueCross is considered confidential and protected by the Privacy Act. The BlueCross Data Center is responsible for appropriate marking and labeling magnetic media. All Medicare data processed by a subsidiary of BlueCross on behalf of Medicare lines of business must be labeled as “CMS Sensitive Information.” All sensitive data stored on tapes and servers are in secure facilities with restricted access.

1.8.7 Configuration Management

The following section defines how the organization shall:

- Establish and maintain baseline configurations and inventories (including hardware, software, firmware, and documentation) throughout development life cycles.
- Establish and enforce security configuration settings for products employed.

Configuration Management (CM) is the responsibility of all BlueCross managers. Such procedures provide a consistent method of communicating, validating, approving, and implementing changes within the production environment. This includes changes to hardware, software, security mechanisms, and processing structure (e.g., application releases, validating, operating environment, voice/data network environment, storage, databases, environmental software, etc.).

ICT NH Configuration Management Plan consists of various procedural steps that all personnel are required to follow for the plan to be operated and maintained properly. ICT NH will adhere to and execute the Compliance Management Process to reflect BlueCross' configuration posture.

1.8.7.1 Inventory

Procedures have been developed, documented, and implemented by each team within ICT NH effectively to document and maintain a current inventory of the information system's constituent components and relevant ownership information. The inventory of information system components, at a minimum, includes the manufacturer's name, model/type, serial number, software license information, version number, location (i.e., physical location and logical position within the information system architecture), and system/component ownership. Additional fields within Integrated Asset Management System (IAMS) are utilized for the specific inventory needs of each team within ICT NH, and those fields are defined within each team's procedures.

The ICT module within IAMS is utilized to update the information system component inventory as an integral part of component installations. IAMS is the central authoritative master inventory of all Non-Host servers and network devices (e.g., routers, switches, and firewalls). All inventory reports, references, and information are considered accurate as of the date and time the information is pulled directly from IAMS.

All information system component inventory procedures are updated as they change, and each team within ICT NH reviews these procedures at least annually.

1.8.8 Maintenance

The following section defines how the organization shall:

- Perform periodic and timely maintenance.
- Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct maintenance.

1.8.8.1 Maintenance Controls

The BlueCross Data Center uses many security controls to monitor the installation and updates to hardware, operating system software, and other system software to ensure that the hardware and software function as expected and that an historical record is maintained of system changes. These security controls are also in place to ensure no configuration changes have been made to the baseline configuration that is unauthorized or outside of the configuration standards set forth by management.

Security baselines follow regulatory standards to meet contractual obligations of BlueCross contract business. These regulatory entities include PGBA DoD Security Technical Implementation Guide (STIG), National Security Agency (NSA) and National Institute of Standards and Technology (NIST) standards, the CMS security guidance found in the Centers for Medicare & Medicaid Services Acceptable Risk Safeguards (CMS ARS), and HIPAA guidelines. Exceptions to these guidelines are either noted in policy or in Alternate Control Documents (ACD) for Medicare and Commercial business and in Mitigation Strategy Report Form (MSR) for PGBA business. The ICT NH Infrastructure/Security Information Management team creates and maintains the ACD and MSR documents. These documents

are reviewed by the line manager and signed by the line manager, Director, and Assistant Vice President (AVP) of ICT NH.

1.8.8.2 Hardware Maintenance

Any changes to hardware equipment or software will be carefully reviewed and validated, and will be scheduled for implementation. Peak workload periods should be avoided for implementation. Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate validation. Maintenance schedules should be distributed and maintained as required by each Line of Business (LOB).

Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations. All maintenance and repair is performed within the BlueCross Data Centers. Devices are not shipped off-site for repair. At least two days advance notification on hardware changes is given to users so that service is not unexpectedly interrupted. During this time, physical checks will be conducted to ensure no physical damage has occurred to cables. Regular and unscheduled hardware maintenance performed is documented. After maintenance is performed, security features are checked to ensure they are functioning properly.

The ICT NH area does not maintain an inventory of redundant hardware. Procedures are in place to handle designated equipment failure. ICT NH maintains appropriate maintenance contracts for critical infrastructure equipment through the manufacturer or an authorized maintenance facility. These contracts are written with response time agreements for hardware failures. Assessments of the critical infrastructure's existing vulnerability, reliability, and threat environment are made at least annually.

1.8.8.3 Network Maintenance

Logical Network Design

If there is a request from a customer of ICT NH Division to implement a new logical network access point, an infrastructure request form is completed by the customer. These forms are monitored by the business group within ICT NH and distributed to the appropriate technical areas.

The technical area will schedule meetings with the necessary departments within ICT NH including the Security Information Management (SIM) team to review the request. During the meetings the feasibility of the request is reviewed. If the request is reasonable and does not pose any security issues in accordance with best practices and regulatory requirements from BlueCross contracts, the most secure method of implementing this access request is formulated.

This proposed method is reviewed by the SIM group and management for their approval prior to implementation.

Simple Network Management Protocol Community String Policy

ICT NH ensures Simple Network Management Protocol (SNMP) community strings are changed from their default values. The SNMP community string age/expiration values are set in accordance with DoD guidance. Additionally, the Information Assurance Manager/System Security Officer (IAM/SSO) will ensure that string creation follows the complexity requirements used when creating user passwords.

ICT NH will restrict access to the SNMP community strings on the devices by placing ACLs that allow authorized IPs to pull SNMP information.

The process for reporting and mitigating known or suspected compromise to the SNMP community string on infrastructure devices will follow the corporate standard incident response and handling procedures. During a computer security incident, individual users, the Compliance department, and Security Specialists (network, Enterprise Server, and facilities areas) will work together to resolve the incident.

The network infrastructure support team will document the SNMP community string for all network infrastructure devices and will follow the necessary procedures for the creation, maintenance, and access to the SNMP community string.

Network Guidelines

1. Operating system controls are configured to disable public read-and-write access to all system files, objects, and directories. Operating system controls are configured to disable public read access to files, objects, and directories that contain sensitive information.
2. Peer-to-Peer communications is not approved within the BlueCross environments.
3. Sessions on systems are also configured to time out after a pre-determined time of inactivity.
4. In order to provide 24/7 support, ICT NH does not restrict users/administrators to log-on hours. Configuration Management (CM) protocols and policies have been developed to ensure a consistent process, and change control documentation is used to establish baselines for the controls to requested changes. A formal systems change request process is strictly followed for any system configuration change. All software changes proceed through a series of steps designed to ensure quality and security.
5. Computer Associate's Unicenter Asset Management (UAM) tool is used to maintain a baseline of systems. The UAM tool actively monitors systems for installed software and hardware to include versioning, manufacturer, type, serial number, patches installed, etc.
6. Segregation of duties is enforced to ensure that only highly qualified associates have access to production libraries. These libraries are used to maintain audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates.
7. Maintenance tools are periodically reviewed to ensure they are running at the latest approved versions. Vendor equipment is reviewed and a virus scan run prior to the equipment being allowed to connect to the network or a BlueCross owned system. In addition, if any diagnostic program is contained on removal media, a virus scan is run on the media in the administrator's workstation prior to being attached to the information system.
8. Regular vulnerability scans are run on network and server devices to ensure no configuration changes have been made to make devices vulnerable to possible hacker type attacks or less secure configuration management requirements.

1.8.8.4 Software Maintenance

System Security Software Management

The BlueCross Data Center installs updates to technical software that have been in distribution by the vendor (beta version) for at least six months. Certain circumstances require the BlueCross Data Center

to use outdated software and the most recent software version. The use of both outdated and most recent software releases requires approval by the AVP of Operations.

An assigned control group performs validation and approval of system software, with compensating controls in place to ensure minimal impact to all users. All changes to the system software must be approved by the AVP of Operations. Once the system software from the testing environment has been validated and approved, an independent library control group migrates it to the production environment.

Management reviews all emergency software changes. Once management approves an emergency change, an Information Systems (I/S) supervisor reviews it and the Operations group validates all changes to ensure proper functionality. To minimize the impact on operations and users, a normal change only occurs on the weekend and only after the change is approved during the Weekly Change/Quality Assurance meeting.

Remote access to the server console is restricted. Only individuals with approved access can issue full operator commands. Access to system software is restricted to personnel with corresponding job responsibilities. Update access is limited to those whose job functions require it. This access is reviewed when necessary or quarterly by ICT NH. Access is revoked whenever there is a status change for users holding these IDs.

Remove Default Programs and Scripts

As a rule, ICT NH groups will not leave any default scripts installed on the servers. If Common Gateway Interface (CGI) scripts must be installed as a requirement by the application, then the scripts must be custom written by the responsible application area.

Currently, any existing scripts that are part of the code base for web applications are controlled through GitHub.

Cleanup after Utility Run

System administrators will perform a system cleanup after all utility runs by deleting all unnecessary files and backup files from the system. Once the AIX utility run is complete, the AIX administrators will delete all text files and any other system/backup files that were created during an AIX utility run. This will ensure that all unnecessary files and backup files created during utility runs are removed from the system.

1.8.9 Alternate Platform Administrative Procedures

1.8.9.1 Request for Network User Accounts

To request a network user account, a member of management must complete and submit the *Network Access - Add/Change/Delete* form via the TSC Self-Service.

1.8.9.2 Request for Departmental Network Access

To request a network departmental (which may include one or more users) account, a member of management must submit the *Network Access - Add/Change/Delete* form via the TSC Self-Service.

1.8.9.3 Network User IDs

A network user id will be assigned to you upon completion of one of the above processes. This User ID is your Employee ID; thus, you must have an Employee ID before requesting a network user ID. Please note that the passwords of these User IDs are not kept in sync.

The first time you sign on, using your assigned network user ID, you will be prompted to change your password. Your new password must be at least 6 characters in length. Your passwords will expire every 45 days.

Network accounts not used for 60 days will be disabled. If there is no response from the user within another 60 days, the account and associated files will be removed from the system.

1.8.9.4 Default Network Resources

All accounts will be limited to 10 Megabytes of disk space for private and shared files. If additional Disk Space is necessary, a member of management must submit the *Home Drive Space Increase/Decrease* form via the TSC Self-Service.

Please note that once an employee has terminated employment, their network account will be disabled and their files backed up. The account and files will be kept for 90 days and then deleted. If you need to access the files of a terminated employee, please complete the appropriate Service Request form available on the TSC Self-Service Portal.

1.9 Risk Assessment

The following section defines how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

1.9.1 Operation Risk Management

ICT NH will use technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and installation of the latest hardware/software patches), and penetration testing to assist in the ongoing review of system security measures and compliance. The ICT NH review includes an annual assessment of security policies and associated procedures.

1.10 Medicare Considerations

1.10.1 Medicare Support Definition

The Centers for Medicare & Medicaid Services (CMS) mandate security requirements for companies working directly for Medicare and subcontractors. Because some areas of I/S subcontract and support Medicare contracts, these areas are subject to the same controls.

For I/S and other areas of BlueCross BlueShield of South Carolina (BlueCross), these controls apply to persons with logical or physical access to Medicare data. Access to the Medicare domains is considered Medicare Support.

Listed below are examples:

- Logical access — Employees who have Medicare log-in ability such as RACF, Active Directory, etc.
- Physical access — Employees with direct physical access to Medicare data and information, such as the Print Center, Data Center and Medicare-restricted areas.

1.10.2 Portable Electronic Media Information Transfer

Medicare Support Cost Center staff are prohibited from transferring Sensitive and Restricted Medicare-related information to portable electronic media (such as CDs, DVDs, diskettes, or tapes) that are not part of the approved backup procedures. If transfer of Medicare information is required, it must be performed by a staff member of Medicare following that area's internal standard procedures.

1.10.3 ARS Control Family Policy and Procedures

The Acceptable Risk Safeguards (ARS) controls that are required by CMS for many of their Medicare contracts are grouped together by subject matter to form Control Families. As a result, the Control Families contain a set of controls that have a common purpose or goal.

1.10.3.1 Provision Description

The controls within each Control Family are sequentially numbered with the first (*01*) control stating that the organization is committed to the Control Family topic.

The *01* common verbiage is as follows:

The organization:

a. Develops, documents, and disseminates to applicable personnel:

1. A *Control Family Subject Matter* policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the *Control Family Subject Matter* policy and associated *Control Family Subject Matter* controls; and

b. Reviews and updates (as necessary) the current:

1. *Control Family Subject Matter* control policy at least every three (3) years; and
2. *Control Family Subject Matter* control procedures at least every three (3) years.

The term *Control Family Subject Matter* used in the common verbiage is replaced with the appropriate terminology for each of the Control Families.

1.10.3.2 Provision Implementation Details

The *01* control wording states that a *policy* should exist to address the need. It has been assumed that the BlueCross Corporate Policies will be the solution. However, this is not the case. The purpose of the BlueCross corporate policies is to address the enterprise-wide common core issues, and not individual contractual needs. Otherwise, the corporation's policies would potentially need to be updated every time when new contracts are obtained containing contractual requirements.

To address the *01* control, a single all-encompassing standard was written.

The organization:

a. Develops, documents, and disseminates to applicable personnel:

A variety of documents are developed documenting the subject matter and are then disseminated to the applicable staff. These documents may include:

- BlueCross Corporate Policies
- Information Systems Standards Manual (ISSM)
- Control Procedures

Each of the document types have update processes that are managed, and the results are announced and housed in a location accessible by all applicable staff.

1. A *Control Family Subject Matter* policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

The BlueCross corporation is committed to producing quality, well-managed results for all of our customers. This is documented within the *Our Values* program throughout BlueCross.

In addition, the methodology utilized by the I/S Division is designed to handle all work efforts and to produce quality results with the correct scope and purpose, involving all necessary roles and clearly defining the involved responsibilities.

Through our contract review and acceptance of the relevant contract, the requirement for compliance is made, and this commitment is translated to the staff through the day-to-day requirement to comply with our corporate policies and also the ISSM/Control Standards.

2. Procedures to facilitate the implementation of the *Control Family Subject Matter* policy and associated *Control Family Subject Matter* controls; and

Control Procedures are currently developed as needed for those controls that involve detailed processes.

b. Reviews and updates (as necessary) the current:

1. *Control Family Subject Matter* control policy at least every three (3) years; and
2. *Control Family Subject Matter* control procedures at least every three (3) years.

Review and update — The BlueCross corporate policies, the ISSM standards, and the Control Procedures are reviewed annually.

1.11 Certificates and Public Key Infrastructure

Public Key Infrastructure (PKI) is the end-to-end administration life cycle of keying material and certificates including the policies, procedures, people, hardware, and software that create, distribute, use, store, and revoke these keys. These keys and certificates ensure that data moves securely between our systems within our security perimeter and beyond while maintaining integrity and confidentiality. This section outlines the specifics about how BlueShield of South Carolina (BlueCross) employs certificates and the guidelines around how they are managed.

1.11.1 Definitions and Summary

The functional benefit of certificates and certificate authorities occur when two entities both trust the same certificate authority as a third party. The establishment and recognition of this third-party trust allows both entities to authenticate each other and/or exchange keys with confidence by validating the certificates signed by that trusted certificate authority without prior knowledge of the other entity or its keys. These entities use the exchanged keys to encrypt communication or to verify authenticity of digital documents, software packages or transactional records between one another.

1.11.1.1 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document that certifies the ownership of a public key by the named subject of the certificate. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified that the certificate's contents are correct. A certificate provides:

- Authentication — Verification of an owner's identity.
- Confidentiality — Protection of information from unauthorized disclosure.
- Data Integrity — Protection of information from unintended modification.
- Non-Repudiation — Prevention of an entity from denying previous actions.
- Key Establishment — Secure establishment of cryptographic keying material between two entities.

1.11.1.2 Certificate Authority

In cryptography, a certificate authority (CA) or certification authority is an entity that stores, signs and issues digital certificates and acts as a trusted third party — trusted by both the subject (owner) of the certificate and the party relying upon the certificate. This trust allows others (relying parties) to confidently rely upon signatures or assertions made by the private key that corresponds to the certified public key.

1.11.1.3 Registration Authority

In cryptography, a registration authority (RA) is an authority in a network that verifies user requests for a digital certificate and authorizes the CA to issue it. The main purpose of an RA is to ensure that the request is legitimate, a user or device is allowed to request a digital certificate from a CA, and the request does not violate security policy or guidelines. While the RA cannot create or issue a certificate, it works as an intermediary for the CA to collect necessary information and to process the following tasks:

- Receive user or device certificate requests
- Confirm the legitimacy of the certificate request
- Validate users or devices
- Authenticate users or devices
- Ensure that the certificate request meets accepted security policies and guidelines
- Revoke credentials if the certificate is no longer valid

1.11.2 Certificate Authorities

BlueCross' official PKI consists of two certificate authority sources: our external certificate authority vendor and our authorized internal certificate authorities. These certificate authorities establish a third-party hierarchy of trust between the various systems and boundaries where BlueCross PKI is utilized. Entities that manage the CA sources can have any number of independent roots or intermediate trust chains within their issuing hierarchy.

1.11.2.1 Trust Stores

All certificate authorities trusted or managed or both by BlueCross must have their trust chain certificates placed in the trust stores of the various systems, services, and devices to ensure proper operation for clients. ICT has placed the trust chains into the stores of the major OS platforms like Windows workstations, Windows servers and Unix servers as appropriate so that they can be leveraged as needed. However, it is the responsibility of the application or certificate owner to leverage the trust stores in place on the OS or establish their own trust chain within their systems or application trust store as required to ensure that their certificates operate properly. ICT can supply any trust chain certificates for BlueCross-authorized PKI if requested.

1.11.2.2 External Certificate Authority

BlueCross selected a commercial vendor that provides externally signed, publicly trusted certificates for interactions with our customers and business partners on our sites, services, and systems inside and outside the organization. Management of the external certificate authority contract, vendor relationship and the availability of the vendors services are the responsibility of Cyber Security Operations (SecOps) under I/S Governance.

1.11.2.3 Internal Certificate Authorities

BlueCross owns and maintains root and intermediate certificate authority infrastructure within our internal networks that provide internally signed, privately trusted certificates for interactions across our internal sites, services, and systems. Management of this internal certificate authority infrastructure and its services are the responsibility of ICT. These internal CAs are officially authorized, documented systems that are designated for this purpose and are present in various network locations or environments to provide functionality to all platforms and technologies within the BlueCross environment as needed. BlueCross CA hierarchy is as follows:

- **Root CA** — The Enterprise root trust anchor for the Corporate Data Center. This certificate authority only issues signing certificates to other authorized CAs in the BlueCross private hierarchy. No endpoint certificates can be issued from this CA.
- **Domain Enroll CAs — BCBSSC Class 1** — Certificate authorities integrated with Microsoft Active Directory for domain member auto-enrollment, one per domain. These cover all Microsoft

Windows workstations and servers that are joined to a domain. Certificates issued from these CAs are referred to as *System Managed* and are automated for enrollment, renewal and provisioning using Active Directory as the registration authority.

- **Manual Enroll CAs — BCBSSC Class 2** — Certificate authorities that support manual enrollment and renewal for non-domain joined assets including applications, appliances, and other systems. Certificates issued from these CAs are referred to as *Manually Managed* and require manual intervention to enroll, renew and provision. Cyber Security Operations performs the role of registration authority, reviewing each request before approval.
- **Device Enroll CAs — BCBSSC Class 3** — Certificate authorities that support device enrollment outside a domain using Network Device Enrollment Service (NDES) or Simple Certificate Enrollment Protocol (SCEP). Certificates issued from these CAs are referred to as *System Managed* and are automated for enrollment, renewal and provisioning using client authentication with NDES/SCEP as the registration authority.
- **Signing or Transactional CAs — BCBSSC Class 4** — Systems or services that do not sign or issue other certificates, but that sign transactions, packages or documents using an authorized certificate for this purpose. While these may or may not be actual CAs in some cases, they are actively signing for other purposes in a similar way to certificate signing. As such, they will be treated as CAs within the BlueCross PKI and fall under the same guidance as a certificate authority.

1.11.2.4 Other Certificate Authorities

There are various other external certificate authorities (public or private) that might be trusted by BlueCross internal systems to conduct business across the organization. These are evaluated on a case-by-case basis and trusted as needed but are not part of the BlueCross authorized PKI environment.

There are other internal certificate authorities deployed and maintained by the various business units and subsidiaries that are used internally for their purposes within their own networks or systems. These CAs may be considered official for their respective purposes within their respective environments, but they are NOT considered part of the formal BlueCross-authorized PKI environment and are not managed or maintained by ICT. These CAs are selectively trusted within the greater BlueCross environment on individual systems as needed.

1.11.2.5 Certificate Revocation Lists

BlueCross provides a Certificate Revocation List (CRL) location in the form of a website for all BlueCross private enterprise CAs in the Corporate Data Center to publish their revocation lists. This location is accessible both externally and internally from all network placements in the Corporate Data Center to permit all clients that trust BlueCross certificates to validate the revocation status of any internally issued certificates on use.

1.11.3 Certificate Categories and Use Cases

At present, BlueCross recognizes five distinct use case categories for digital certificates within the organization.

1.11.3.1 Externally Issued Certificates

An externally issued certificate is a digital certificate issued by BlueCross from our external, publicly trusted, commercial certificate provider and placed on BlueCross sites, services, or systems. The identity described in the certificate (endpoint) is distinct and separate from the entity issuing the certificate (authority). All certificates issued from this external authority will chain back to the external issuing root. Externally issued certificates are required for all Uniform Resource Locators (URLs) that are publicly accessible (such as from the internet) and require Public Key Encryption. Externally signed certificates may also be used for systems integration with external business partners or internally for compliance or customer requirements. Only approved external certificate authority vendors may be used.

1.11.3.2 Internally Issued Certificates

An internally issued certificate is a digital certificate issued by BlueCross from our internal, privately trusted, enterprise certificate authority, owned and operated by BlueCross. The identity described in the certificate is distinct and separate from the entity issuing the certificate. All certificates issued from an internal authority will chain back to the appropriate internal issuing root. Internally issued certificates may be used where the URL is not publicly presented, and requirements do not mandate a publicly signed certificate. These certificates are not publicly trusted. They are only trusted within the BlueCross network boundary or by BlueCross-maintained equipment or systems.

1.11.3.3 Self-Signed Certificates

A self-signed certificate is a digital certificate issued by a device, service, or site to itself (the same device, service, or site). The identity described within the certificate is the same as the entity issuing the certificate and does not chain back to a third-party issuing root to validate the certificate is authentic. Self-signed certificates should be avoided where possible, and explicitly not be used where an identity is being authenticated or validated as there is no trusted third party to validate the identity presented. Self-signed certificates may be used to encrypt network traffic between two devices or systems where independent/third-party authentication is not required. These certificates are not trusted by any entity (internal or external) except the entity that issued it. Explicit action would be necessary to share the certificate with another entity for the purpose of trust.

1.11.3.4 Vendor-Issued Certificates

A vendor-issued certificate is a digital certificate issued by a vendor that is embedded into a vendor supplied product, service or system utilized by BlueCross. These certificates can be either be publicly trusted from an external authority, or self-signed, but typically are under sole control of the vendor and cannot be altered by BlueCross independently. Depending on the issuer, they may or may not be trusted by other BlueCross systems or customers.

1.11.3.5 Third-Party-Issued Certificates

A third-party-issued certificate is a digital certificate issued to BlueCross and applied to BlueCross sites, services or systems. The certificate originates from either an external business partner, a customer or either of their designated certificate providers, or another certificate provider not under BlueCross contract or management. These certificates may or may not be publicly trusted or trusted by other BlueCross systems or customers.

1.11.4 Certificate Keys

Certificates consist of several data elements that must be periodically maintained or updated to keep the certificate current, along with its keying material. This keying material, or asymmetric key pair, are two separate but relationally linked keys, a public key and a private key.

The public key of a certificate contains only public non-sensitive data. This key can be transferred over the network or internet with no security risk. The public key is normally transferred to the CA to be signed and returned to the owner and is passed to the relying party for use in validation and to complete authentication of the owner.

Private keys should only be held by the certificate owner. They are highly sensitive and should be secured appropriately. The private key is normally used to decrypt information encrypted by the public key. Transmission over the network or internet should be limited, and any files containing private keys should be secured with a password and appropriate controls to prevent unauthorized access or compromise.

1.11.4.1 Key Storage and Protection

Appropriate protection of the keying material on the target system or application is the responsibility of the certificate owner. The certificate owner will ensure that they are familiar with the location of certificates and keying material within their designated application or system and understand the technical or administrative controls and vendor guidance applicable to these locations for proper protection of the keying material.

Private keys should be protected from unauthorized access using file system permissions, strong key store passwords and/or other technical and administrative controls applicable to the application, system, or technology where the key resides for the applicable security boundary. This protection should employ the principle of least privilege and restrict access to these keys only to certificate owners or their delegates that require this access to support the keys or their configuration. Care must be taken to only store private keys in appropriate locations (like OS or application key stores) with required protections in place. Private keys should never be stored on network file shares or in unrestricted file systems.

1.11.4.2 Key Generation and Distribution

Generation of the keying material for a certificate should take place where possible on the endpoint or system where the certificate or private key or both will reside when in service. This approach reduces unnecessary access by administrators and transit of the sensitive keying material over the network. When the situation requires it, transmission of the private key over the network or to an external party may be necessary. When this occurs, the administrator must ensure that the temporary private key file is encrypted using a strong password when it leaves the origin point (downloaded from the keystore, etc.) If the file must be transmitted over the internet, the password protected keying material must be transmitted using SECURE email or equivalent secure file transfer service. The password for the private key file should never be included in the communication along with the file. The password should only be provided through a separate communication (verbally where possible or at least through a separate, secure email to the recipient). The transmission of the protected keying material files and their passwords should be addressed to authorized recipients only and never sent to distribution lists or additional parties for awareness. All temporary, private key files used for transmission should be removed or deleted once the transmission is completed, and the key is in place.

In situations where BlueCross cannot generate the keying material internally and is a recipient of private keys from an external source or a third party, the receiving administrator should ensure that the file is password protected upon receipt. They should also ensure that the password to the file is provided in a separate communication, confirm that the keys are intended for the purpose identified, and place the private keys into service under the technical or administrative controls of the target system as dictated by the security boundary of said system. All temporary private key files used for transmission should be removed or deleted once the transmission is completed, and the key is in place.

For systems that have their certificates and keying material automatically generated and provisioned by the Certificate Management tool, a copy of the private key may also be retained in that supporting system. This additional copy of the private key will be secured using appropriate controls within the Certificate Management tool. Access to this copy should be restricted to the certificate owner and their identified delegates, simlar to the target system where the private key resides.

1.11.4.3 Key Rotation

Certificate private keys are considered secret. Compromise of these keys can result in the loss of data or exposure of sensitive information. Private keys are rotated as part of the expiration and subsequent renewal of a certificate when it reaches the end of its validity period. The validity period for a given certificate can vary depending on several factors but typically range between one to three years. Consideration should be given to renewing certificates more frequently to minimize exposure should they be leaked or stolen. Financial and operational impacts to a system from renewal/rotation of a certificate must be weighed if considering regular rotation before normal expiration. Renewing externally issued certificates before the expiration dates also incurs additional vendor costs.

Private keys should always be rotated or certificates renewed when events occur that would put the keys at risk. These events include, but are not limited to:

- A private key (or the system/application on which the private key operates) is suspected of compromise or found to be improperly secured.
- A private key/certificate supplied by an external party is reported as being compromised.
- A private key is found to be mishandled in transmission or stored in an insecure location.
- Staff with privileged access to the key or key store are terminated or leave the company.

NOTE If system or key compromise is suspected, a security incident ticket should be opened via TSC Self-Service as soon as possible.

1.11.4.4 Key Recovery

Certificate owners shall determine if their systems, applications, or any cryptographic techniques used require that the keying material be available for recovery if lost or is otherwise unavailable. A certificate owner who determines that keying material recovery is a requirement should address the continued accessibility or recovery of the keying material within the target system's operational procedures or disaster recovery plan where the keying material is discussed. If keying material recovery becomes necessary for anyone other than the certificate owner, the certificate owner will seek the approval of a director or above prior to starting the keying material recovery.

While the Certificate Management tool may possess an additional copy of keying material under some use cases, the Certificate Management tool should not be considered a primary recovery source for keying material on target systems.

1.11.5 Certifcate Inventory Management

Certificate Management is an enterprise-wide process that provides end-to-end self-service capabilities for all I/S and business areas that manage certificate inventory. The goal of the Certificate Management process is to provide certificate inventory management, certificate discovery and ownership assignment, which is accomplished through the Certificate Management tool.

1.11.5.1 System Managed vs. People Managed

Some certificates are automatically issued, signed, deployed, and renewed by vendor products. These are classified at BlueCross as *System Managed*. By the numbers, the System Managed category accounts for most certificates in use across BlueCross BlueShield of South Carolina systems. In contrast, certificates that are manually obtained and deployed are categorized as *People Managed*. These require thoughtful consideration as to the role certificates play within the system and must be covered by a documented, Certificate Management process.

For People Managed certificates (including self-signed certificates), the entire life cycle of a certificate is the responsibility of the support organization for the device, application, appliance or product on which the certificate is used. This includes the following certificate life cycle events:

- Request
- Installation
- Revocation
- Compliance
- Replacement or Renewal (when validity ends for any reason)

1.11.5.2 Workflow Review Standards

Workflow reviews are performed to verify the validity of the certificate, to ensure that there are no adverse impacts to other processes that determine decisions for business outcomes for various teams, and to ensure that there are no imminent threats to our network. A comprehensive list of approval criteria can be found in area desk procedures.

The three workflows that are featured in the Certificate Management process for new, existing and revoked certificate inventory are listed below along with the areas or roles responsible for them and their responsibilities:

- **Certificate Oversight Workflow** — Certificate Oversight is responsible for the overall business and system impacts regarding certificate decisions for their respective organizational area. This process participant is engaged when a workflow is initiated and decisions as to certificate needs, to renew, not to renew, and renovation are needed.
- **Security/Technical Workflow** — Security is responsible for managing risk and providing guidance.
- **Operational Impact Workflow** — The certificate owner is responsible for ensuring the deployment of or the approval to provision the certificate to the device, application, or system.

1.11.5.3 Certificate Management Process — New, Existing and Revoked Certificates

The life cycle of the Certificate Management process (Figure 1-11) consists of the following stages and describes how the certificate inventory will be enrolled, deployed, managed, and revoked within the process.

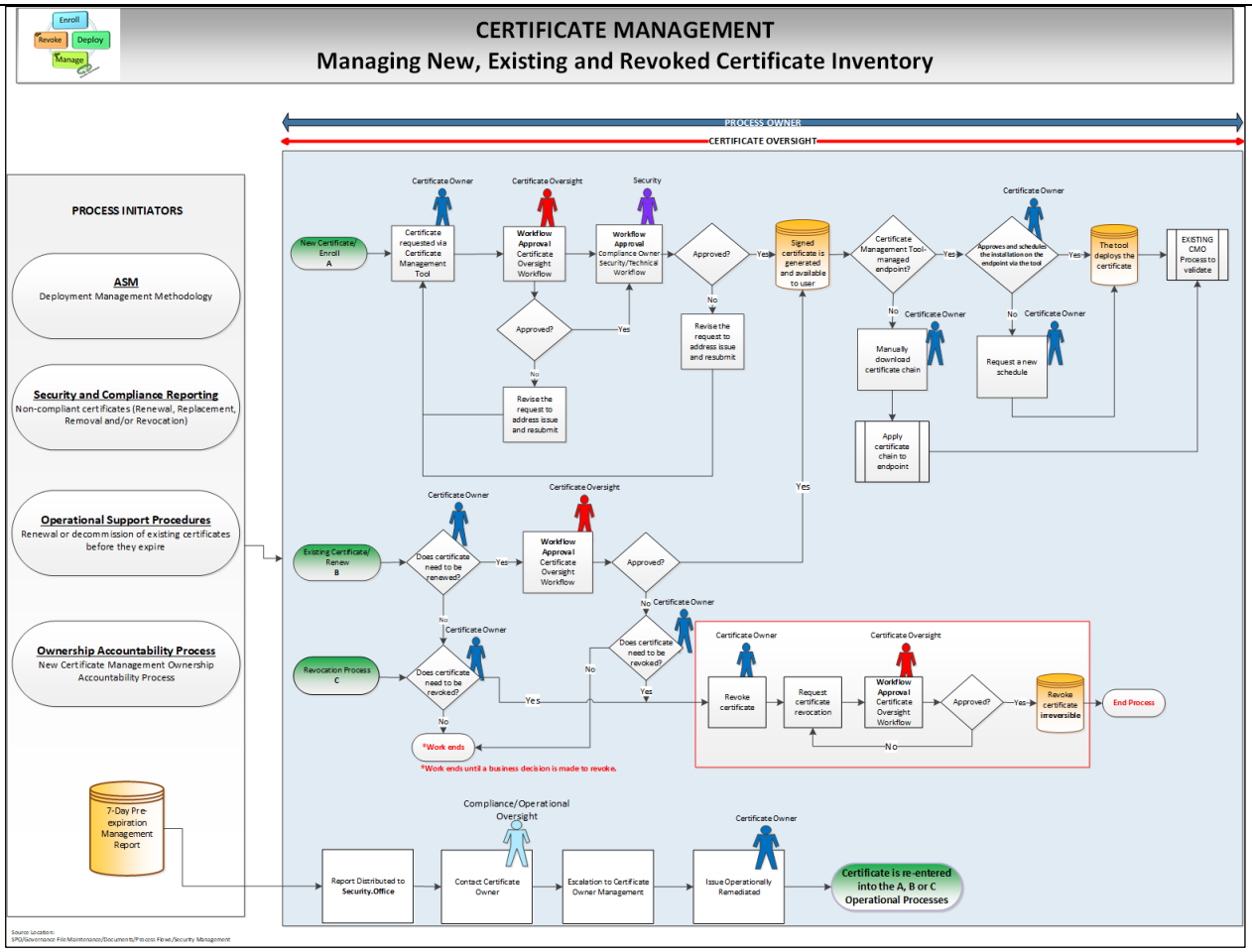


Figure 1-11 Certificate Management — Managing New, Existing and Revoked Certificate Inventory

Enroll

- Certificate enrollment must be engaged by one of the following initiators:
- Deployment Management Methodology
- Security and Compliance Reporting
    - Non-compliant certificates (renewal, replacement, removal and/or revocation)
- Operational Support Procedures

  - Renewal or decommission of existing certificates before they expire.

- Ownership Accountability Process

Once initiated, a new certificate enrollment is requested through the Certificate Management tool. When the request is submitted, the Certificate Oversight workflow is engaged to review the request for approval. The approval decision is based on the workflow standard criteria stated above and additional, more detailed approval criteria documented for this workflow and maintained by the Certificate Oversight team. Certificate approval is based on the following factors, but not limited to: the domain name is owned or managed or both by BlueCross BlueShield of South Carolina (BlueCross), users are authorized to request certificates under this domain name, certificate details are valid, etc. A comprehensive list of approval criteria can be found in area desk procedures. If the enrollment request is denied, the request is revised to address the issues (e.g., invalid domain name requested, improper URL, incorrect Certificate Authority requested for the use case, etc.) and is resubmitted by the certificate owner.

After the Certificate Oversight workflow approval, the Security team is engaged for a Security/Technical review and approval. The approval decision is based on the workflow standard criteria stated above and additional, more detailed approval criteria documented for this workflow and maintained by the Security Operations team. If the enrollment request is denied, the request is revised to address the issues and is resubmitted by the certificate owner. If approval is granted, the signed certificate is generated. The certificate is then available to the user, and the deployment process begins.

The above process initiators must also precede the request to renew an existing certificate. Once the process is initiated, the certificate owner decides if the certificate is needed and needs to be renewed. Certificate Oversight workflow is engaged to review the request for approval. The approval decision is based on the workflow standard criteria stated above and additional, more detailed approval criteria documented for this workflow and maintained by the Certificate Oversight team. If approval is granted, the signed certificate is generated. The certificate is then available to the user, and the deployment process begins.

If the certificate owner decides that the existing certificate should not be renewed or Certificate Oversight rejects the renewal request or both, the certificate owner should initiate the revocation process.

Deploy

After the signed certificate is generated and available to the user and if the endpoint is integrated with the Certificate Management tool, the certificate owner schedules the installation on the endpoint via that tool. The scheduling and approval by the certificate owner occur in the same step. The Certificate Management tool deploys the certificate, and the process progresses to the Change Management Office (CMO) process to validate. If the scheduled deployment must be altered, the certificate owner must repeat the scheduling workflow in the tool.

When the endpoint is not integrated with the Certificate Management tool, the certificate owner performs a manual download of the certificate and chain, then manually applies them to the endpoint. The process continues to the CMO to validate.

Manage

In addition to managing new and existing certificates, the Certificate Management process also manages ownership accountability.

Revoke

Once the certificate progresses to the Revocation Process, the certificate owner makes a request to revoke the certificate. Certificate Oversight workflow is engaged to review the request for approval. The approval decision is based on the workflow standard criteria stated above and additional, more detailed approval criteria documented for this workflow and maintained by the Certificate Oversight team. If approval is granted, the certificate is revoked in the Certificate Management tool, and the process ends.

NOTE The certificate revocation process is irreversible.

If the Certificate Oversight workflow does not generate an approval, the certificate owner is responsible for resolving any issues with the request. Once those issues are resolved, the request for revocation can be resubmitted.

The entire Certificate Management process is overseen by System Experts, Technology Owners, and Certificate Oversight. The Process Owner ensures that the end-to-end process is executed as defined, collaborates with impacted areas, and identifies gaps for process improvement.

NOTE Expired or unused certificates no longer meet security or operational requirements and should be revoked.

7-Day Pre-expiration Management Report

The purpose of the 7-Day Pre-expiration Management Report is to allow time for resolution prior to certificate expiration and possible outages. When the report is distributed to Compliance Oversight, the certificate owner will be contacted, followed by an escalation to certificate owner management. Upon successful operational remediation, the certificate is re-entered into the Operational Process.

1.11.5.4 Certificate Management Process — Ownership Accountability

The Certificate Management Ownership Accountability Process (Figure 1-12) can be initiated by one or more of the following activities.

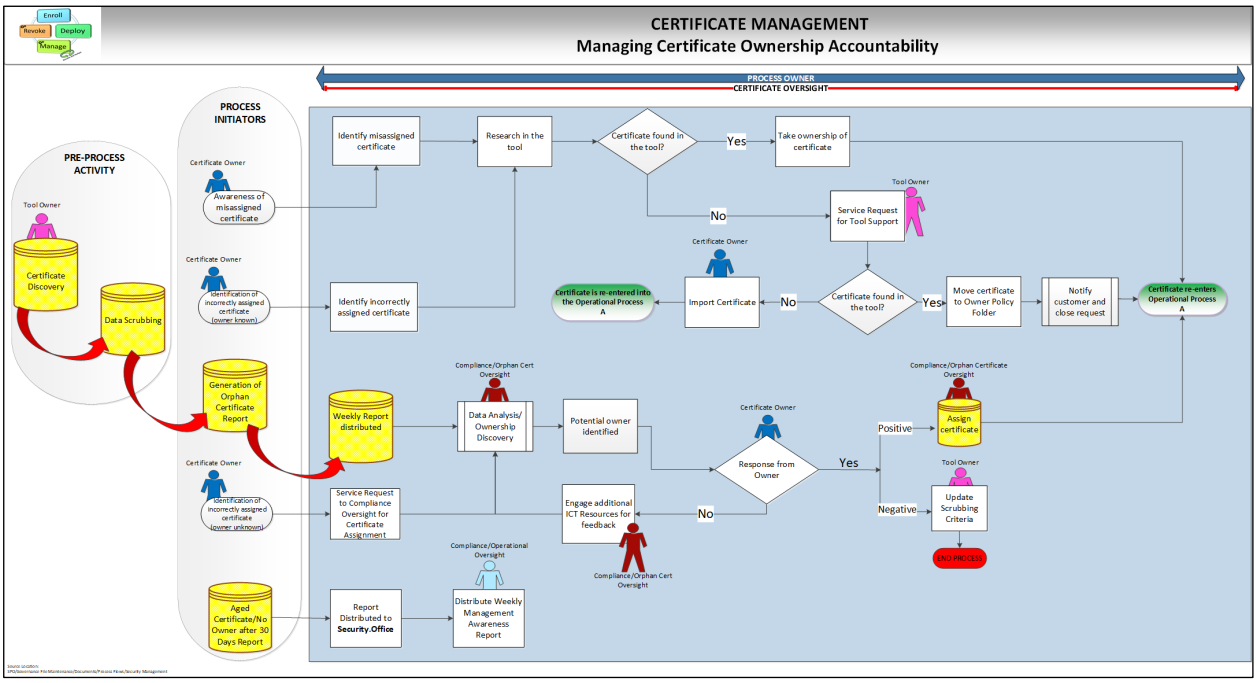


Figure 1-12 Certificate Management — Managing Certificate Ownership and Accountability

Awareness of a Misassigned Certificate

A certificate owner may discover certificates that they own are missing from their assigned inventory or misassigned within the Certificate Management tool. After discovering that the certificate is not correctly assigned, the certificate owner searches the Certificate Management tool to locate the certificate. If the certificate is located, the certificate owner takes ownership of certificate, and the certificate re-enters the Operational Process as a new or existing certificate.

If the certificate owner is unable to locate the certificate in the Certificate Management tool, a Service Request is submitted to Tool Support. If the certificate is then located, it is moved to the Owner Policy folder, the customer is notified, the ticket is closed, and the certificate re-enters the Operational Process as a new or existing certificate.

If Tool Support is unable to locate the certificate within the Certificate Management tool, additional research is done by the Incident Management process until the certificate is located. This resolution is dependent on desktop procedures and an operational health assessment. Once the certificate is located, the customer is notified, and the ticket is closed. The certificate re-enters the Operational Process as a new or existing certificate.

Identification of Incorrectly Assigned Certificate (Certificate Owner Known)

When an incorrectly assigned certificate is identified and the certificate owner is known, a Service Request is submitted to Tool Support. Once the certificate is located, it is moved to the Owner Policy folder, the customer is notified, the ticket is closed, and the certificate re-enters the Operational Process as a new or existing certificate.

Generation of Orphan Certificate Report

The Orphan Certificate Report is generated and distributed to a predetermined list of recipients. From this report, orphan certificates are identified, and the Data Analysis/Ownership Discovery sub-process is engaged. If the certificate owner is not confirmed, the Data Analysis/Ownership Discovery sub-process is re-engaged until a certificate owner confirmation is obtained. Once the certificate owner is confirmed, Compliance Oversight will make the certificate assignment via the Certificate Management tool, and the customer will be notified. The certificate re-enters the Operational Process as a new or existing certificate.

Identification of Incorrectly Assigned Certificate (Certificate Owner is Unknown)

When an incorrectly assigned certificate is identified and the certificate owner is unknown, a Service Request is submitted to the Compliance Oversight to have the certificate correctly assigned. The Data Analysis/Ownership Discovery sub-process is then engaged. If the certificate owner is not confirmed, the Data Analysis/Ownership Discovery sub-process is re-engaged until a certificate owner confirmation is obtained. Once the certificate owner is confirmed, Compliance Oversight will make the certificate assignment via the Certificate Management tool, and the customer will be notified. The certificate re-enters the Operational Process as a new or existing certificate.

Aged Certificate/No Owner after 30 Days Report

The purpose of the Aged Certificate/No Owner after 30 Days Report is to keep management abreast of the certificates that have not been assigned to an owner after 30 days. When the report is distributed to Compliance Oversight, this information will be distributed weekly to management via a Management Awareness Report.

1.11.5.5 Certificate Management — Ownership and Responsibility

The Certificate Management process engages many area participants with various ownership responsibilities. The list below describes the process participants, their tasks, and the BlueCross I/S Governance roles associated with each process participant:

- **Certificate Oversight** — Accountable for the overall business and system impacts regarding certificate decisions for their respective organizational area. This process participant is engaged when a workflow is initiated and decisions as to certificate needs, to renew, not to renew and renovation are needed. The I/S Governance roles for these process participants can be any management-assigned role within Operational Support, System Support or Network Services.
- **Certificate Owners** — Ensure that the operational processes are carried out for certificates and provide day-to-day system support. The I/S Governance roles for these process participants are Operational Support Analyst, System Support Analyst and Network Operations Analyst.
- **Compliance/Orphan Certificate Oversight** — Ensures that all certificates are assigned to an owner within the Certificate Management tool. This will be the responsibility of Asset Services.
- **Compliance/Operational Oversight** — Ensures that management is made aware of all unassigned certificates that are 30 days or older. This will be the responsibility of Compliance Oversight & Risk Reporting.
- **Process Owner** — Ensures that the operational process is executed as defined, collaborates with impacted areas, and identifies gaps for process improvement. The I/S Governance roles for these process participants are System Expert and Technology Owner.

- **Security** — Responsible for managing risk and providing guidance. The I/S Governance role for this process participant is any management-assigned role within the Cybersecurity Operations Center.
- **Tool Owner** — Ensures that all necessary tool modifications are carried out. The I/S Governance role for this process participant is any management-assigned role within Infrastructure Services or Operational Support.

1.12 Production Data Updates by I/S Personnel

Three conditions must be met in order for an I/S staff member to update data for a production system outside of the application:

1. Approval by a Customer Data Owner — A Customer Data Owner will approve any update of a production system's data. A documented request made by a Customer Data Owner to update the data is considered approval. A "Customer Data Owner" is defined as someone in the business operations unit responsible for the data.

   Exception: Customer approval is not required to correct technical issues, such as spaces or low values.

2. Review — The person applying the update will conduct a review of the proposed actions with a technical peer and document concurrence. This is to ensure that "two sets of eyes" have reviewed the change prior to it being applied to the production environment.
3. Documentation — The person applying the update will store the evidence of the approval, review concurrence and the execution of the update so it is available on request.

The preferred technique for updating a production system's data outside of the application is a "P" Job.

1.13 Personnel Security

The following section defines how the organization shall:

- Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria.
- Ensure that systems are protected during and after personnel actions such as terminations and transfers.
- Employ formal sanctions for personnel failing to comply with security policies and procedures.

1.13.1 Personnel Screening

Potential candidates for employment with BlueCross BlueShield of South Carolina (BlueCross) undergo a background check. This check covers personal history/employment and criminal investigations. BlueCross gathers background information through a variety of official agencies. The two official agencies used include the South Carolina Law Enforcement Division (SLED) and Acxiom for information outside of South Carolina. For select personnel, background reinvestigations are conducted every five years.

1.13.1.1 Personnel Segregation

Least Privilege

Each individual with access to major applications is held responsible for all of his or her actions on the system. User activity is auditable so that any security breaches can be reconstructed and traced to the responsible individual. Integrity controls are also used to ensure that information is not modified or destroyed in an unauthorized manner. Each user is granted the most restrictive set of privileges needed to perform their authorized tasks. These integrity controls help to limit the damage that results from accident, error or unauthorized use.

Segregation of Duties

Job descriptions are based on the position's required skill set and technical expertise level for successful job performance. These job descriptions reflect the tasks performed by each associate and are compliant with the segregation of duties principle. Security software is used to restrict access. Access is based on the user's role and business need. Justification for client/server access requires management approval along with business justification. For instance, in addition to System Administrators having access to the Web server, the Web Application Support team also needs access. However, the Web Application Support team only has administrative level access to the Web Unit, System, and Quality Assurance (QA) servers. They are restricted to read-only access to the Production Web servers. The access capabilities of systems programmers are periodically reviewed for propriety to ensure that access permissions correspond with job duties. Application managers and operational management review individual access rights to ensure proper segregation of duties.

When a new Administrator is hired or if a person's job responsibilities change and administration is added to that person's responsibilities, their manager must submit the *Network Access - Add/Change/Delete* form via the TSC Self-Service to request the person's new access. The owner of the admin group receives the request and approves or denies the request. If approved, Data Security Administration (DSA) (or appropriate team) provisions the access.

Administrator-level access groups are reviewed and maintained on an active listing of approved administrators on a weekly basis as part of the Seven-Day Administrator Review process and as needed.

The use of unique and separate accounts helps to ensure that administrative activities are kept separate from non-administrative activities. System Administrators use unique UserIDs and passwords to perform administrator functions. These UserIDs are not shared with anyone and are different from the administrator's own personal UserID.

1.13.1.2 Personnel Accountability

Each associate is provided with a unique employee/contractor identification number (ID) and personal identification number (PIN) in order to work at BlueCross. The ID number is electronically embedded in each associate's access badge and is used to further identify the associate to Resource Access Control Facility (RACF), network and applications, and throughout the BlueCross facility.

To enforce individual accountability, the physical security department uses the C*CURE 800® integrated security management monitoring system for issuing and tracking building access cards. C*CURE 800® is a product of Sensormatic/Software House and uses a 37-bit proximity card. For each associate, the C*CURE 800® system records a photograph, name, employee ID, security badge number and authorized building access for each associate.

1.13.1.3 Employee Confidentiality

All associates and contractors with access to sensitive claim information are required to sign the BlueCross Employee Confidentiality Statement Agreement form. This agreement is reviewed and signed on the first day of employment and annually during the Corporate Compliance Training Program.

Employees are required to guard sensitive information and not allow sensitive information to be revealed to unauthorized individuals or sources. Release of sensitive information is strictly prohibited and is not to be released to unknown or known individuals that do not have a need to know (social engineering). Employees are taught to enter access codes, PINs, and passwords in a way that prohibits retrieval through shoulder surfing. To prevent eavesdropping, sensitive information is encrypted when sending via email.

1.14 Awareness and Training

The following section defines how the organization shall:

- Ensure that systems managers and users are made aware of the security risks associated with their activities.
- Ensure that personnel are adequately trained to carry out their duties and responsibilities.

1.14.1 Security Awareness and ComplianceTraining

All BlueCross BlueShield of South Carolina (BlueCross) workforce members are required to receive security awareness and compliance training both during New Employee Orientation, and annually thereafter. Security awareness training information is provided in the Corporate Compliance training material, which is made available to all workforce members during in-person or computer-based training. The Corporate Compliance training includes HIPAA Privacy and Security training, training on Fraud and Abuse topics, training on adherence to Federal Laws, and training on Corporate Rules of Behavior, which BlueCross calls *Our Values*. Workforce members acknowledge receipt and completion of their training and agree to comply with the Corporate Code of Conduct, which includes Privacy and Security Rules, the Corporate Rules of Behavior, and other laws that affect our business. Monthly corporate email security reminders are also distributed to all user email accounts to make users aware of current security issues, threats, and exploits.

In addition to security awareness training, some corporate Lines of Business (LOBs) require additional role-based training for specific purposes. Corporate LOBs define the requirements for training, and I/S workforce members are assigned training as needed. Some teams in I/S may require specific training applicable only to their areas that must be completed prior to performing assigned duties.

1.14.2 Professional Training

To meet and maintain certification requirements, Management will ensure that all I/S workforce members keep up to date with the latest professional training as it relates to their role and responsibilities.

Chapter 2 System Security

This chapter contains standards that are applicable for information security used at BlueCross BlueShield of South Carolina.

2.1 System Administrator Access

System Administrators are individuals who have been granted an advanced level of access with elevated permissions to I/S resources such as mainframe systems, servers and workstations. With these elevated rights, System Administrators may be given limited or total control of the operating system and files on I/S resources to perform configuration changes. System Administrators must take extreme care when using System Administrator accounts.

System Administrator access is a privilege provided to individuals who require elevated access in order to do their jobs effectively. The access is requested as described in section *Requesting System Administrator Access* below.

2.1.1 System Administrator Active Directory (A Dash) Accounts

System Administrators who require local administrator access to workstations are provided a special Active Directory administrator account that gives elevated permissions to local I/S resources. This account is separate from their regular corporate account. This account provides special access to administrator functions and activities on a local workstation, but does not permit the ability to access email or internet to minimize exposure to security threats. The account is for use when conducting their System Administrator responsibilities. Abuse or misuse of this account will not be allowed. Use of the account will follow the corporate System Administrator responsibilities and standards provided in the sections *System Administrator Responsibilities* and *System Administrator Standards* below.

The naming convention for the ID for System Administrator Active Directory accounts will have *A-* in the first two characters of the account ID followed by the administrator's employee ID (e.g., *A-1234*). This is commonly known as an *A Dash account*. Passwords for an A Dash account ID will not be changed using the password synchronization tool.

2.1.2 System Administrator Responsibilities

System Administrators may be responsible for the following during the performance of their duties:

- Create, modify, and access domain and local user accounts and groups
- Replace, install or uninstall new infrastructure hardware and/or infrastructure software
- Modify operating system configurations and settings (e.g., network settings, access control, file resource sharing, local firewall, services configuration, etc.)
- Modify or upgrade the operating system
- Install company-approved applications and utility programs
- Configure audit logs and auditing behavior
- Configure boundary protection rules.

This is not a complete list of all of the responsibilities. These responsibilities should only be used as part of an approved work effort, support or maintenance function, or as directed by I/S management. I/S management should keep these tasks in mind when requesting System Administrator access for an individual.

2.1.3 System Administrator Standards

Individuals who are granted any level of System Administrator access must adhere to the following standards and sign the appropriate attestation form.

- Must be familiar with corporate policies with an emphasis on Corporate Policies 65004–65010.
- Must manage/control I/S resources in a manner that complies with the intent of Corporate Policy and other guidelines published by the corporate I/S organization.
- Must safeguard user privacy and related data housed on I/S resources.
- Must safeguard company resources housed on I/S resources. This includes timely maintenance, data protection and resource availability.
- Will be held accountable for the I/S resources they have access to and manage or control.
- Will not download or install any unapproved or unauthorized software on any I/S resource.
- Will only use their administrative account for required administrator functions.
- Will only update those system configurations and settings required as part of a work task and as part of a work effort. Modification of settings for personal convenience is prohibited.
- Will not create new local administrator accounts, assign local administrator rights or modify user access levels of an existing account on any I/S resource unless authorized.
- Will not modify the content of system, security event, or audit log files.
- Will not delete any system, security event, or audit log files.
- Will not modify, stop, or disable any systems security resources or software such as anti-virus, anti-malware or monitoring programs unless authorized.

Any exceptions to the above standards can only be made with management authorization. Individuals who violate these standards or abuse the access will have their administrator rights removed immediately and will be subject to disciplinary action, up to and including termination.

NOTE Users of company-issued laptops will be granted local System Administrator access to the device for the purpose of configuring peripheral devices that are needed for business reasons, such as printers, scanners, projectors, etc., when off-site, and will also adhere to the standards listed above in this section.

2.1.4 Requesting System Administrator Access

System Administrator access is an advanced level of access with elevated permissions to I/S resources such as mainframe systems, servers and workstations. All requests require business justification, management and AVP approval.

- Managers of individuals requiring System Administrator access will provide justification for the access and complete the *System Administrator Access – Create Account* Service Request form located on TSC Self-Service.
- Managers of individuals requiring access to local infrastructure devices such as local workstations will provide justification for access and complete the *Local Admin Rights on PC* Service Request form located on TSC Self-Service. Once submitted, the individual's responsible AVP will be contacted by the ICT Deployment Team to approve the access request.

- All System Administrators must successfully complete the current *System Admin Access Training* IST CBT course located on the Learning Management System (LMS) prior to being granted System Administrator rights.
- All personnel must review and attest to adherence to corporate standards on the appropriate attestation forms: *System Administrator Access Guidelines and Responsibilities, System Administrator Access Guidelines and Responsibilities for External Users*. The attestation documents will be included with the CBT and attested annually.
- The Administrator Group Owners will review and approve the System Administrator Access Service Request prior to Data Security granting access.

2.1.5 Removal of System Administrator Access

As stated above, System Administrators are individuals who have been granted an advanced level of access with elevated permissions to I/S resources such as mainframe systems, servers and workstations. System Administrator access is tightly controlled and restricted to those who have the need. As responsibilities change for System Administrators due to a change in responsibilities, departmental transfer, punitive action and company termination, System Administrator access will be removed through the following processes:

- To remove System Administrator access from their staff, managers will complete the TSC Self-Service request form *System Administrator Access - Delete Account*.
- To remove Administrator access to local infrastructure devices from their staff, managers will complete the TSC Self-Service request form *Local Admin Rights on PC*.
- Removal of System Administrator access can also be requested by I/S security teams or senior management due to punitive action as a result of a violation of standards.

2.1.6 Periodic Reviews

The Information Systems division will conduct management reviews of System Administrator access at a minimum of once every seven days as part of the Seven-Day Administrator (Seven-Day Admin) Review as well as on an as-needed basis.

2.1.6.1 Technology System Administrator Definitions

The platforms, technologies and Seven-Day Admin discovery rules involved in these periodic reviews are listed below (Table 2-1). The seven-day admin discovery rule defines the admin rules for the type of accounts discovered in the seven-day admin process.

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
Host	z/OS	• Any user with UPDATE or higher access to system datasets • Any user with the SPECIAL or OPERATOR attribute at the group or system level in RACF
Non-Host (Unix)	RSA	Any account that has an admin role as defined by the RSA Security Console
Non-Host (Unix)	UNIX	Any user who is provided the ability to run a command as root with sudo via the sudoers file, which has not been deemed "non-administrative" by the Platform team. This access can be granted either as: • a direct user definition • a group definition A non-administrative command (or command alias) will be flagged within the sudoers file as such. The criteria of an administrative command should be commands that include, but are not limited to, the ability to do the following: • Modify access to the system • Install/remove system components (e.g., SW, libraries, Modules, files, directories) • Modify privileged system settings (e.g., kernel, network, storage, memory) • Modify privilege file system attributes (e.g., files, folders, file systems, mount points) • Start/Stop privileged processes (e.g, services, applications, scheduled tasks)
Non-Host z/Linux	z/Linux	Any user who can execute a privilege task via the "sudo" command as listed in a sudoers policy. SUDO allows for the execution of privileged commands as the "root" (superuser) account or to a user account that has an UID of "0." This also applies to local and remote users

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
		(LDAP/RACF) that are defined in the sudoers file. Policies defined in the sudoers file include, but are not limited to, the following administrative attributes: • Modify access to the system • Install/remove system components (e.g., SW, libraries, Modules, files, directories) • Modify privileged system settings (e.g., kernel, network, storage, memory) • Modify privilege file system attributes (e.g., files, folders, file systems, mount points) • Start/Stop privileged processes (e.g., services, applications, scheduled tasks) Note: A user who has the ability to log on to a z/Linux system does not have an administrative attribute. A user will inherit an administrative attribute when defined in a sudoers policy. Today, user accounts inherit their sudoers policy through their connected groups and, in very limited application, some service accounts for automation/security are explicitly defined in the sudoers definition.
Data/Voice Network (Data)	Terminal Access Controller Access Control System (TACACS)	Local or Remote AAA accounts for network devices that have write permissions to make changes to device configurations are considered administrator.
Data/Voice Network (Data)	Network (Local)	A user that has write permissions to make changes to device configurations is considered an administrator
Non-Host (Windows)	Active Directory	An account that permits elevated access within the directory service to perform the following tasks: • Creating/deleting/updating users, groups, and computer

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
		objects (workstation and servers). (Account/server operators) • Creating/deleting/updating organizational units • Group policy management (Group policy creator owners) • Domain management roles (Built-in groups for admin access: Domain, Schema, and Enterprise Admins) • Domain local administrators' group (<domain>\administrators)
Non-Host (Windows) Workstation	Windows (Local)	An administrator on Windows Server can be considered as one that possess any of the following characteristics: 1. A local account, local group (members within), domain account, and/or domain group (members within) that is a member of the local administrators group on a Windows Server device. 2. A local account, local group (members within), domain account, and/or domain group (members within) that can perform any of the following tasks: a. Adding or removing groups b. Adding or removing user accounts c. Backing up and restoring folders and files d. Changing date and time settings and synchronizing with an internet time server e. Changing Ease of Access administrative settings f. Changing power settings;

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
		turning off Windows features; uninstalling, changing or repairing a program g. Making changes to file or folder permissions, commonly referred to as an access control list (ACL) h. Making changes to files in folders that standard users don't have permissions for (e.g., %SystemRoot% or %ProgramFiles%) i. Making changes to system-wide settings j. Changing a user's account name or type k. Changing remote, system protection or advanced system settings l. Changing settings for Windows Firewall m. Changing user account controls (UAC) settings n. Configuring Windows Update o. Creating a new account or deleting a user account p. Elevating privileges to an administrator when prompted to accept UAC q. Installing ActiveX controls r. Installing and uninstalling applications outside of the %USERPROFILE% (e.g., C:\Users\[logged in user]) folder and its subfolders. Most of the time this is in %APPDATA% (e.g., C:\Users\[logged in user]\AppData). By default, this is a hidden folder. Chrome's and Firefox's installer ask for admin

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
		rights during install. If given, Chrome will install in the Program Files folder and be usable for all users. If denied, Chrome will install in the %APPDATA% folder instead and only be usable by the current user. s. Installing and uninstalling display languages t. Installing device drivers u. Merging and deleting network locations v. Modifying network information w. Restoring backed-up system files x. Running an application as an administrator y. Running Disk Defragmenter or System Restore z. Running Registry Editor aa. Running Task Scheduler bb. Running the Windows Experience Index assessment cc. Troubleshooting audio recording and playing, hardware/devices, and power use dd. Turning on Guest account ee. Turning on network discovery, file and printer sharing, Public folder sharing, turning off password protected sharing or turning on media streaming ff. Turning on or clearing logs in Remote Access Preferences gg. Viewing or changing another user's folders and files 3. A local account, local group (members within), domain

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
		account, and/or domain group (members within) that is granted any of the following user right assignments: a. Access Credential Manager as a trusted caller b. Act as part of the operating system c. Adjust memory quotas for a process d. Back up files and directories e. Change the system time f. Create a pagefile g. Create a token object h. Create global objects i. Create permanent, shared objects j. Create symbolic links k. Debug programs l. Enable computer and user accounts to be trusted for delegation m. Force shutdown from a remote system n. Generate security audits o. Impersonate a client after authentication p. Load and unload device drivers q. Lock pages in memory r. Log on as a batch job s. Log on locally t. Log on as a service u. Manage auditing and security log v. Modify an object label w. Modify firmware environment values x. Obtain an impersonation token for another user in the same session y. Perform volume maintenance tasks z. Profile single process aa. Profile system performance

Technology System Administrator Definitions

Architectural Platform	Seven-Day Admin Technology Area	Seven-Day Admin Discovery Rule
		bb. Remove computer from docking station cc. Replace a process-level token dd. Restore files and directories ee. Shut down the system ff. Synchronize directory service data gg. Take ownership of files or other objects
Host	zVM	• Any user with UPDATE or higher access to system datasets • Any user with the SPECIAL or OPERATOR attribute at the group or system level in RACF
Cloud	Azure AD	An administrator in Azure AD is a user whose roles assignment allows them to: 1. Create or manage user, service accounts and groups 2. Make configuration and policy changes within any of the Azure Services and Microsoft 365 products (e.g., Exchange Online, SharePoint Online, Teams) 3. Read account, tenant or product configuration information (e.g., sign-in logs, security alerting/reports, compliance dashboards)

Table 2-1 Technology System Administrator Definitions

2.2 Cloud Administrator Access

Cloud Administrators are a type of system administrator for privileged access to cloud services or applications. With these elevated rights, Cloud Administrators may be given limited or total control of the cloud account or tenant and resources within to perform configuration changes.

Cloud Administrator access is a privilege provided to individuals who require elevated access in order to do their jobs effectively within authorized cloud services. Use of these Cloud Administrator accounts will follow the existing System Administrator Standards found in the section *System Administrator Standards* above.

2.2.1 Requesting Cloud Administrator Access

Cloud Administrators are individuals who have been granted an advanced level of access with elevated permissions to I/S resources in the cloud such as Azure, Amazon Web Services (AWS) or other approved cloud services or applications. All requests require business justification, management and AVP approval along with the following:

- Manager of individuals requiring Cloud Administrator access will provide justification for the access and complete the *Cloud Administrator Access – Create/Change/Delete* form located on TSC Self-Service.
- All Cloud Administrators must successfully complete the current System Administration Access Training IST CBT course located on the Learning Management System (LMS) and the *SEC Privileged User Security Series: Secure Cloud Administration* LMS Course prior to being granted Cloud Administrator rights.
- All personnel must review and attest to adherence to corporate standards on the appropriate attestation forms: *System Administrator Access Guidelines and Responsibilities* and *System Administrator Access Guidelines and Responsibilities for External Users*. The attestation documents will be included with the CBT and attested annually.
- The Cloud Administrator Group owners will review and approve the Cloud Administrator membership via the quarterly access review process.

2.2.2 Removal of Cloud Administrator Access

Cloud Administrator access is tightly controlled and restricted to those who have the need. As responsibilities change for Cloud Administrators due to change in responsibilities, departmental transfer, punitive action and company termination, Cloud Administrator access will be removed through the following processes:

- The manager of individuals requiring Cloud Administrator access will provide justification for the access and complete the *Cloud Administrator Access – Create/Change/Delete* form located on TSC Self-Service.
- Removal of Cloud Administrator access can also be requested by I/S security teams or senior management due to punitive action as a result of a violation of standards.
- Removal of Cloud Administrator access can be the result of the 90-day Access Review process and will be done automatically as a result of manager access recertification.

2.2.3 Authenticating Cloud Administrator Accounts

Due to the nature and accessibility of Cloud Administrator accounts from anywhere and under all conditions, Cloud Administrator accounts must require multi-factor authentication (MFA) as a part of the logon process. MFA is required at each logon, at the start of each new session and regardless of location using Azure MFA with the Microsoft Authenticator Mobile App. When authenticating to cloud sessions, if idle for more than 15 minutes, the Cloud Administrator will be prompted to re-authenticate with MFA.

2.3 Management Class

2.3.1 Organizational Security Program Management

2.3.1.1 BlueCross BlueShield of South Carolina Data Center ICT NH Overview

The BlueCross BlueShield of South Carolina (BlueCross) Data Center is designed to be used by job functions and supporting programs such as healthcare finders, enrollment and billing personnel, claim examiners, correspondence personnel, nurses and medical directors.

Assets Covered

All major applications are hosted in the BlueCross Data Center on an Enterprise Server composed of IBM Z-series computers. ICT NH maintains an inventory of all assets that can be retrieved upon request.

Distributed applications reside on Non-Host servers in the BlueCross Data Center. Typically, only one major application resides on each server in the Non-Host environment.

2.3.1.2 Applicable Laws or Regulations Affecting the System

The following laws, regulations, and policies are applicable to this system or application:

1. Public Law 93-579, The Privacy Act of 1974, as amended http://www.dodig.mil/Resources/PolicyReferences/Privacy/pa1974.pdf.
2. Public Law 99-474, Computer Fraud and Abuse Act of 1986 http://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1213.pdf.
3. Public Law 100-235, Computer Security Act of 1987 http://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf.
4. Public Law 104-106, Clinger-Cohen Act of 1996, (formerly called the Information Technology Management Reform Act) http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf.
5. Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, Electronic Freedom of Information Act of 1996 http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.
6. Public Law 106-398, October 30, 2000, National Defense Authorization for Fiscal Year 2001, which includes the Government Information Security Reform Act (GISRA) of 2000 http://www.gpo.gov/fdsys/pkg/PLAW-106publ398/pdf/PLAW-106publ398.pdf.
7. Public Law 104-13, Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35 http://www.gpo.gov/fdsys/pkg/PLAW-104publ13/pdf/PLAW-104publ13.pdf.
8. Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996 http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.
9. Public Law 74-271, Social Security Act, as amended, §1816, Use of public agencies or private organizations to facilitate payment to providers of services http://legcounsel.house.gov/Comps/Social%20Security%20Act-TITLE%20XI.pdf.
10. Public Law 74-271, Social Security Act, as amended, §1842, Use of carriers for administration of benefits http://legcounsel.house.gov/Comps/Social%20Security%20Act-TITLE%20XI.pdf.
11. Presidential Decision Directive/NSC-63 (PDD 63), Policy on Critical Infrastructure Protection, May 22, 1998 http://www.fas.org/irp/offdocs/paper598.htm.

12. Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control, June 21, 1995. http://www.whitehouse.gov/omb/circulars/index.html.
13. OMB Circular No. A-127, Financial Management Systems, Transmittal 2, June 10, 1999 http://www.whitehouse.gov/omb/circulars/index.html.
14. OMB Circular A-130, Management of Federal Information Resources, Transmittal 4, November 28, 2000 http://www.whitehouse.gov/omb/circulars/index.html.
15. Security of Federal Automated Information Resources, Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, November 28, 2000. http://www.whitehouse.gov/omb/circulars/index.html.
16. Federal Information Security Management Act of 2002 (FISMA) http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
17. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM), Volume I, Financial Statement Audits, January 1999 http://www.gao.gov/special.pubs/ai12.19.6.pdf.
18. IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, June 2000. http://www.irs.gov/pub/irs-pdf/p1075.pdf.
19. Gramm-Leach-Bliley Act of 1999, November 12, 1999 http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.
20. Department of Defense (DoD) Directive 8500.01E Information Assurance dated October 24, 2002 (Certified Current as of April 23, 2007) http://dodcio.defense.gov/Portals/0/Documents/DIEA/850001p.pdf.
21. DoD Instruction 8500.2 Information Assurance Implementation dated February 6, 2003 http://www.cac.mil/docs/DoDD-8500.2.pdf.
22. Defense Information Systems Agency Security Technical Implementation Guides. (Available online at http://iase.disa.mil/stigs/Pages/index.aspx.)
23. Military Health System Automated Information System (AIS) Security Policy Manual.
24. National Automated Clearing House Association (NACHA) Automated Clearing House (ACH) Rules Compliance — https://www.nacha.org/content/compliance.

2.3.2 Access Control

The following section defines how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

2.3.2.1 System User Authorization

Authorization for associates to access Enterprise Server, Active Directory, Web Servers and secured application resources is based on an associate's job role. Access to resources must be requested, authorized (need-to-know), and approved by the associate's manager and organization management.

ICT NH uses Active Directory Group Policy to configure users work environments for options on their local computer, domain, and Security Information Management (SIM) settings. The Active Directory Group Policy enforces the required security options as defined by ICT NH. ICT NH administrators remove and change access to the system when notified by managers.

Access to Web servers is gained through a KVM solution. The security surrounding this access involves a firewall rule request for the individual's workstation IP address that has to be approved by management and Active Directory rights for server account access.

2.3.2.2 Access Control Lists

Access Control Lists (ACLs) are used to protect all objects, to include directories, files, printers, volumes, etc. Before a complete access control framework or policy is defined, the system data and process model needs to be completed. This information is then used to define which users or groups of users should have access to what information. Some general ACL fundamentals are defined below with the inclusion of object ACLs for the operating system and database management.

General ACL guidance includes the following direction:

1. Build in existing groups if possible. If this is not possible, define a new group. Do not use special accesses as they may cause functional problems.
2. Limit permissions for "write," "delete," "change," and "take ownership."
3. Group common information into directories. Use directory permission to protect rather than using individual file protections. This makes the management of information easier.
4. Use volumes to separate data. For example, put the operating system, database management system, and executive software on separate volumes. This allows for increased access control.
5. Limit access to the operating system and the database to a minimal number of users.
6. Group information by domain user groups.
7. In general, never give the "group everyone" access to anything.

2.3.2.3 Active Directory Group Creation

The customer initiates requests for group creation through an electronic form requiring management approval. The form is automatically sent to the Corporate Audit department for processing and approval. The approved request is forwarded to ICT NH for processing.

ICT NH reviews the request for completeness and accuracy and validates that it meets SIM standards. If the request meets the criteria outlined above, ICT NH then creates the group in the appropriate container and populates the groups with the requested user accounts.

After the group is created, the technician adds a description to the group that documents the purpose of the group and associated rights. The technician also adds his or her initials to the group so its creation can be tracked.

Once the request is completed, it is transferred back to SIM for customer notification.

2.3.2.4 Warning Banners and Password Warning

A warning banner appears on all BlueCross users' workstations' opening screens stating that the system is for authorized use only and that activity will be monitored when accessing protected Enterprise Server regions and networks. See Figure 2-1 and Figure 2-2 on the next page.

BlueCross BlueShield of South Carolina WARNING STATEMENT

This is a BlueCross BlueShield of South Carolina computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized use. BCBSSC computer systems may be monitored for all lawful purposes, to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this BlueCross BlueShield of South Carolina computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or adverse action. Use of this system constitutes consent to monitoring for these purposes.

Figure 2-1 BlueCross Warning Statement

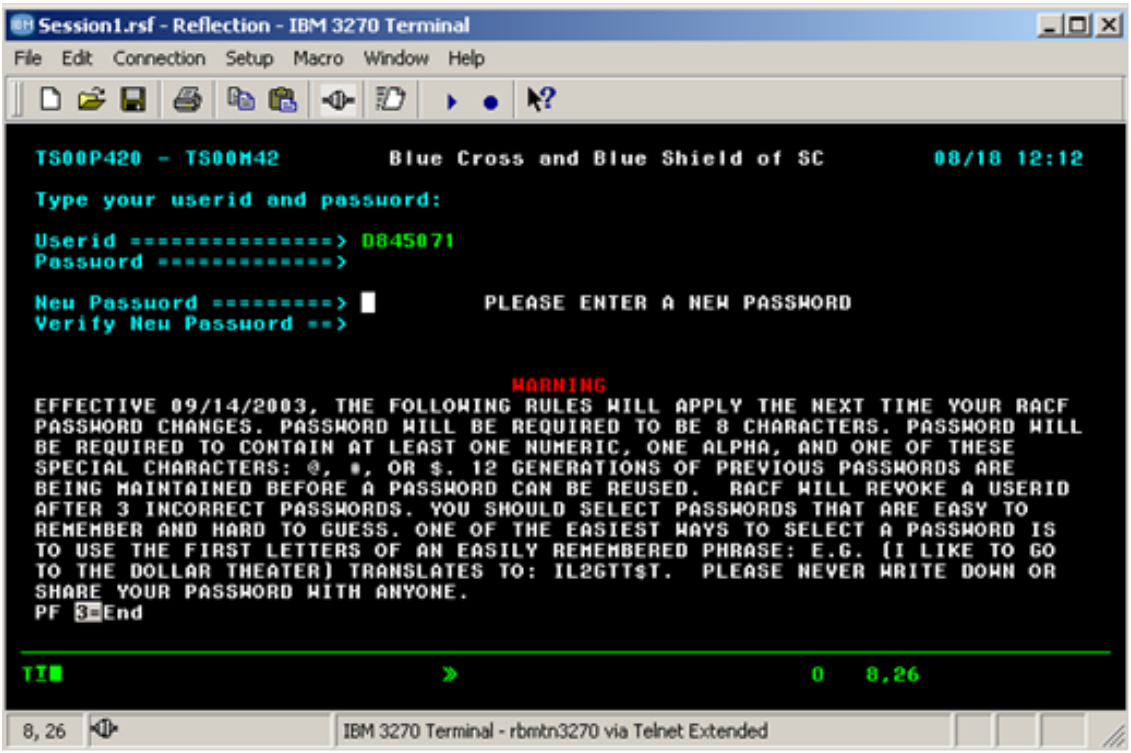


Figure 2-2 RACF Password Warning Used to Access VTAM

2.3.3 Audit and Accountability

The following section defines how the organization shall:

- Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
- Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

2.3.3.1 Audit Activities

SIM systems maintain audit trails. The following activities related to the user and administrator are recorded:

1. Unsuccessful and successful access attempts
2. File related activities (Open/Delete/Modify) against sensitive information
3. Success or failure to complete one of these events
4. ID, date/time of the event, and where the event was initiated
5. Corrective Action Plan progress
6. All program movement for application software
7. New software installs and updates
8. Hardware and Software failures
9. Physical Security Activities

2.3.3.2 Audit Trail Use

Decisions to maintain audit trails and the level of detail for the audits are based on:

1. Value or sensitivity of data and resources affected
2. Type of environment
3. Legal and regulatory requirements

2.3.3.3 Audit Trail Policies and Procedures

Cybersecurity Operations (SecOps) utilizes multiple automated enterprise security products to provide dynamic network monitoring and notification. Security analysts monitor email alerts and management consoles daily to identify abnormalities in server and network device logs.

The SecOps Security Information and Event Management (SIEM) system is being utilized to collect logs from all servers and network devices in the Medicare and PGBA enclaves including the Intrusion Detection System (IDS) sensors, Firewalls and McAfee ePolicy Orchestrator (EPO) for Virus and end-point security. These logs are aggregated and reviewed daily by security analysts. Security analysts monitor events in real time from the SIEM system console and review scheduled reports as required.

Logs are retained for 90 days live, and one year in archive in the SIEM system.

All systems deployed in the Medicare and PGBA enclaves must be configured to transmit audit logs to the SIEM system solution.

CMS Audit-Logging Information

All systems that contain or transmit Centers for Medicare & Medicaid Service (CMS) data, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to provide answers to the following:

1. What activity was performed.
2. Who/what performed the activity.
3. Where the activity occurred.
4. What system type/OS the activity occurred on (Oracle, Sybase, MySQL, DB2).
5. When the activity occurred.
6. What tools the activity was performed with.
7. The status (success vs. failure), outcome, or result of the activity.

CMS Log Creation

Logs will be created whenever any of the activities listed below are requested by a system. Auditable events are reviewed and updated annually or as new requirements are released. Guidelines for log creation are listed below:

1. Create, read, update, or delete any confidential information, including confidential authentication information such as passwords.
2. Create, update, or delete information not covered in #1.
3. Initiate a network connection.
4. Accept a network connection.
5. Provide user authentication/authorization for the above activities including user login and logout.
6. Grant, modify, or revoke access rights including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes.
7. Include system, network, or services configuration changes, including installation of software patches and updates or other installed software changes.
8. Include application process startup, shutdown, or restart.
9. Include system shutdown, system reboot and system errors.
10. Include:
    a. Application process abort, failure or abnormal end, especially due to resource exhaustion or exceeding resource limits or thresholds (CPU, memory, network connections, network bandwidth, disk space or other resources)
    b. Network services such as Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS) failures or hardware faults.
11. Include detection of suspicious/malicious activity from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system or anti-spyware system.

2.3.3.4 Network Device Syslog Auditing

BlueCross uses CiscoWorks for managing Cisco networks and devices. Daily audit reports are generated from CiscoWorks and reviewed by the Infrastructure/Information Security Management team.

CiscoWorks components used at BlueCross include the following:

1. CiscoView — Provides a visual display of the Cisco device.
2. Resource Manager Essentials — Device tracking with network monitoring and fault data, deployment for software images and configuration displays for Cisco routers and Catalyst switches. Provides change control and central syslog collection.
3. Campus Manager — Provides graphical views of network topology and end-user information.
4. Device Fault Manager — Provides data fault analysis for Cisco devices.
5. Internet Performance Monitor — Measures the latency and availability of IP networks on a hop-by-hop (router-to-router) basis.

2.3.3.5 AIX SetUID, SetGID, and World Writable File Auditing

SetUID/SetGID Review

The Compliance and Security Information Management Team (CSIMT) maintains a list of acceptable SetUID and SetGID files and conducts periodic reviews to ensure that no additional files are present. If additional files are discovered, they will be investigated to determine the operational or business need. If the additions are acceptable, they will be added to the list of current SetUID and SetGID files. If the files are found to have no operational or business functions, CSIMT will submit a Request for Change (RFC) to have the rights/privileges changed.

World Writable File Review

CSIMT reviews the business requirements for all world writable files on all UNIX systems and compares them against a list of files, maintained by the relevant System Administrator, needing these permissions. A periodic review is done to check for any additional world writable files. If additional files are discovered, they will be investigated to determine the operational or business need. If CSIMT finds no operational or business need, an RFC will be submitted to have the world writable files and their access permissions removed. If an operational or business need exists, those files with their access permissions will be added to the list of approved world writable files.

Z/LINUX

CSIMT reviews the business requirements for all access to files on all z/Linux systems and compares them against a list of files, maintained by the relevant System Administrator, needing these permissions. A periodic review is performed to check for any additional file accesses. If additional files are discovered, they will be investigated to determine the operational or business need. If CSIMT finds no operational or business need, an RFC will be submitted to have the files and their access permissions removed. If an operational or business need exists, those files with their access permissions will be added to the approved list.

2.3.4 System and Communications Protection

The following section defines how the organization shall:

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

2.3.4.1 Remote Users and Dial-Up Controls

External/Remote Access Policies and Controls

RSA SecurID is the corporate solution for remote access authentication at BlueCross, due to its two-factor user authentication properties. In a two-factor authentication session, the user is required to enter an RSA user name and — in lieu of a password — a PIN plus the current token code from his or her RSA SecurID authentication device. The agent transmits the information to the RSA ACE/Server software, which approves access when the information is validated.

Remote access is enabled through Virtual Private Network (VPN) links, using authorized VPN client software. Encryption standards are used in combination with password authentication and certificate-based authentication or additional authentication protection (e.g., token-based, biometric). Secure management protocols are enabled through VPN links if connected to a network, and Remote Administration is used. Encryption standards are used in combination with password authentication protection (e.g., token-based, biometric).

2.3.4.2 Dial-Up Policy

Workstations with dial-up access generate a unique identifier code before connection is completed. BlueCross deploys many dial-up modems for troubleshooting and access to certain systems. The following guidelines are to be adhered to by all employees in regards to dial-up modems.

Modem Installation Policy

1. All requests for Remote Access System (RAS) Access require a Business Justification to be sent to ICT NH Operations.
2. All modems are to be kept disconnected unless requested for use by authorized personnel or vendors. If modems must remain powered up then they are placed behind the Authentication, Authorization and Accounting (AAA) device of the SecureLogix telephony firewall (TeleWall). The AAA device provides an additional layer of security because the person wishing to connect to the modem must first dial an 800 number and supply a UserID and password. If the authentication credentials are correct then the TeleWall will open the specified modem port for a pre-set amount of time. The person can then dial the modem number and connect as normal.
3. Before connecting, the technician will request a timeframe for which the modem will be used and an hourly figure must be provided. Modems will not be left on overnight unless deemed absolutely necessary and approved by senior ICT NH management. If additional time is needed beyond the original request, requests must be made before the designated disconnect time.

Modem Configuration Policy

1. All users/vendors accessing assets through modems must have a unique UserID that allows them to connect to the designated systems. Passwords must meet minimum corporate security guidelines. Any switched user accounts must be logged and tracked as well. UserIDs are not to be shared.
2. All RAS activities are to be audited on the local asset. Upon completion of the session, all logs pertaining to the session will be sent to the appropriate security staff.
3. All systems will be set to disconnect any session that has three unsuccessful log-in attempts.

Dial-In Modem Use

1. The respective applications area is responsible for any activity on BlueCross assets performed by an Application Vendor.
2. In the event of a violation, the following are appropriate actions to be taken by ICT NH staff:
   a. Initial Violation will result in notification of management and revocation of rights until a management response is received.
   b. Subsequent violations will result in permanent revocation of rights, and the incident will be turned over to the Corporate Compliance Department for official review and resolution, up to and including termination.

Modem Applications Policy

Traffic from Network Modem applications is to be dictated by the requirements of the project or device to which the modem is attached so that all of the requirements of the project or device are satisfied without compromising security policy.

2.3.4.3 Internet/Intranet Policy and Controls

Please refer to BlueCross Corporate Policy 65004 — Information Security Policies, which applies to all BlueCross employees, subsidiaries, agents, and contractors who have internet accounts. ICT NH, at any time and upon request (by Human Resources, or Corporate Compliance), can generate a report using the corporate web URL filtering solution to audit what internet sites users have visited.

Internet services available from within the BlueCross data network are implemented and administered by the BlueCross ICT Network Operations.

2.3.4.4 Wireless Access

Wireless Access Points, including mobile WiFi (MiFi) and smart phones acting as wireless access points, are not allowed on BlueCross property without sufficient business justification and the explicit authorization of the CIO or the chairperson of the Security Council.

All approved wireless access points must be secured by SecOps. Even if approved to be on the premises, these wireless access points may not be connected to the internal BlueCross network.

SecOps maintains a list of approved wireless access points. Wireless scans are conducted on a quarterly basis to identify any unauthorized wireless access points.

2.3.4.5 Internet Security

The internet connection at BlueCross is based on the CMS internet Architectural guidelines for creating the three-tier environment supporting 128-bit Secured Sockets Layer (SSL) encryption.

2.3.4.6 Secure Shell Sessions

Secure Shell (SSH) is a network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary. SSH will be used for all remote access to network equipment where possible.

2.3.4.7 Wide Area Network Access Controls

BlueCross ICT NH has a hardware signature-based IDS system integrated into its corporate LAN/ WAN that monitors, logs, alerts on all activities. It is also used to protect the WAN from unauthorized system penetration, internet threats, and vulnerabilities. These devices are strategically placed on the network to monitor all internal and external activities on a 24-hour per day, seven days per week basis. Internal and external questionable activities are reviewed, investigated, and reported. Systems support alarm features to provide immediate notification of predefined events.

2.3.4.8 Public Access Controls

BlueCross provides a variety of information to providers and beneficiaries, including Directory Smart® application authentication, and credit card payments via the internet. Information is provided to properly identify registered users of Web applications. Users must be authenticated before receiving any information or service and are restricted to information appropriate for that user. All users establish standard IP connections to the internet/intranet servers; no direct connections are supported. Connected users are presented with an appropriate menu of available applications. After authentication by the selected application, the user can receive data selected by the application and presented in the form of Web pages. The user is not allowed direct access to any data.

2.3.4.9 Test Scripts/Results Controls

ICT NH runs various scripts to validate the effectiveness of security controls. These test scripts include penetration testing and ID testing. Penetration testing is used to detect any unauthorized modem(s) or other vulnerabilities on the network, and ID testing is used to identify IDs that are not being used or IDs that are at least 90 days old. Results from these tests are used to correct any inaccuracies or errors in the access control tables, and detect expired IDs.

2.3.4.10 Service/Protocol Controls

Services/Protocols in use with BlueCross include:

1. LDAP — Used for Windows Domain Controllers, Solaris, Cognos, and the corporate web URL filtering solution application services. Domain Controllers currently run LDAPv3 as defined by standards and require anonymous binds to the RootDSE. The RootDSE does not contain any

sensitive information, and anonymous binds are not granted to the remaining portions of the directory.
2. Remote Desktop Services — Used for Citrix application publishing services.
3. DNS — Used for Domain Name resolution services.
4. SNMP — Used for monitoring/alerting services.
5. Application Layer Gateway Service — Application Layer Gateway Service is a component of the Windows OS. It is required if the user uses a third-party firewall or Internet Connection Sharing (ICS) to connect to the internet. Do not end this program in task manager — the user will lose all internet connectivity until next restart or login.
6. Application Management — Provides software installation services, such as Assign, Publish, and Remove. This service processes requests to enumerate, install, and remove applications deployed via a corporate network.
7. ASP.NET State Service — ASP.NET State Service provides support for out-of-process session states for ASP. ASP has a concept of session state — a listing of values associated with the client session is accessible from ASP pages through the session property. There are three options provided to store session data: In process, SQL database, and out-of-process. The ASP State Service stores session data out-of-process. The service communicates with ASP using sockets.
8. Cluster Service — Server clusters provide high availability and scalability for mission-critical applications such as databases, messaging systems, and file and print services. If one of the nodes in a cluster becomes unavailable either due to planned downtime for maintenance or unplanned downtime due to failure of a node, the operating system or an application; another node takes over to provide the service to the end-user — a process known as failover. When failover occurs, users who are accessing the cluster service continue to access the service, and are unaware that it is now being provided from a different server (node).
9. COM+ System Application — The COM+ system application Hosts COM+ services and manages COM+ application configuration and tracking.
10. DHCP Server — The DHCP Server service allocates IP addresses and allows the advanced configuration of network settings such as DNS servers, WINS servers to DHCP clients automatically.
11. Error Reporting Service — The Error Reporting Service provides an infrastructure for collecting, storing and reporting kernel mode, operating system and application faults to Microsoft. Error reporting helps Microsoft track and address errors. The user can configure error reporting to send Microsoft specific error information and to generate reports for operating system errors, Windows component errors or program errors. An operating system error causes the computer to display a blue screen with error codes. A program or component error causes the program or component to stop working.
12. Help and Support — The help service supports the Help and Support Center application and enables communication between the client application and the help data it accesses. This includes access to stores and services such as the taxonomy database that contains metadata and information about the help topics, the support automation framework that enables data collection for registered support providers, user history and preference information, and the search engine manager. When a user is interacting with the Help and Support Center features like search, index, table of contents, and so on, the service allows for a data transaction that supports all of these features.
13. Human Interface Device Access — This service provides generic access to specific functions contained within controls collections on Human Interface Devices (HID). It enables the use of predefined hot buttons on keyboards, remote controls and other multimedia devices.
14. HTTP SSL — Enables Internet Information Services (IIS) to perform Secure Sockets Layer (SSL) functions. SSL is a proposed open standard for establishing a secure communications channel to prevent the interception of critical information, such as credit card numbers. Primarily, it enables secure electronic financial transactions on the World Wide Web, although it is designed

to work on other internet services as well. If IIS is not installed, the HTTP SSL service will depend on the HTTP driver to perform SSL functions. HTTPS is also used to securely connect to the Cisco firewall Adaptive Security Device Manager (ASDM) application to perform administrative tasks. Access to the ASDM application is restricted to the specific IP addresses of the network support staff workstations.

15. Transport Layer Security (TLS) — TLS is used by HTTPS and other network protocols for encryption. TLS 1.3 is the latest version of the TLS protocol.
16. IIS Admin Service — Allows administration of Web and File Transfer Protocol (FTP) services through the Internet Information Services snap-in.
17. Distributed Link Tracking Client — The Microsoft Distributed Transaction Coordinator (MS DTC) is a transaction manager that allows client applications to include several different sources of data in one transaction.
18. FTP Publishing Service — FTP service used internally.
19. Message Queuing — A messaging infrastructure and development tool for creating distributed messaging applications for Windows. Such applications can communicate across heterogeneous networks and can send messages between computers that may be temporarily unable to connect to each other.
20. MSSQLServerADHelper — This service helps Microsoft SQL Server and Microsoft SQL Server Analysis Services to publish information in Active Directory when SQL Server Service and Analysis Server Service are not running under LocalSystem account. This service is dynamically started by an instance of SQL Server or Analysis Manager when needed. The service is stopped as soon as it has completed its work. This service should always be run from LocalSystem account and should not be started manually from the console.
21. Remote Access Auto Connection Manager — Manages dial-up and virtual private network (VPN) connections from your computer to the internet or other remote networks. When the user double-clicks a connection in the Network Connections folder and selects the Connect button, the Remote Access Connection Manager service dials the connection (or sends a VPN connection request) and handles subsequent negotiations with the remote access server in order to set up the connection.
22. Remote Desktop Help Session Manager — Manages and controls the Remote Assistance feature within the Help and Support Center application (helpctr.exe).
23. Resultant Set of Policy Provider —Enables the user to connect to a Windows domain controller, access the Windows Management Instrumentation (WMI) database for that computer, and simulate RSoP for Group Policy settings that would be applied to a user or computer located in Active Directory on a Windows 2000 or later domain.
24. Special Administration Console Helper — The user can use the Special Administration Console (SAC) Helper to perform remote management tasks if the Windows Server family operating system stops functioning due to a Stop error message.
25. Task Scheduler — The Task Scheduler service allows the user to perform automated tasks on a computer. Using Task Scheduler, the user can schedule any script, program, or document to run at a time that is most convenient for them.
26. Secondary Logon — The Secondary Logon service allows the user to create processes in the context of different security principals. Common use of this service is for administrators, who may log on as a restricted user and use the service to temporarily run an application as an administrator.
27. Shell Hardware Detection — AutoPlay is a feature that detects content such as pictures, music, or video files on removable media and removable devices. AutoPlay then automatically launches applications to play or display that content. This simplifies the use of specialized peripheral devices such as MP3 players and digital photo readers. It also makes it easier for users who are unfamiliar with the software needed to access various content types.

28. Simple Network Management Protocol (SNMP) Service — Allows incoming SNMP requests to be serviced by the local computer. SNMP includes agents that monitor activity in network devices and report to the network console workstation. SNMP provides a method of managing network Hosts such as workstation or server computers, routers, bridges, and hubs from a centrally located computer running network management software. SNMP performs management services by using a distributed architecture of management systems and agents.
29. Cisco Discovery Protocol (CDP) — CDP is a Cisco proprietary protocol that runs on Cisco-manufactured equipment including routers, access servers, bridges, and switches, hereafter referred to as network devices. To advertise their existence to other network devices that are directly connected via Layer 2 on the network, network devices use CDP. Each network device that has CDP enabled maintains a table of its neighbors. Network Services uses CDP to gather information on each network device and its neighbors. If CDP is not enabled on a network device, network services will not be able to discover its neighbors and build a topology of the network. CiscoWorks Campus Manager reads the CdpCacheEntry table from CISCO-CDP-MIB via SNMP to learn the neighbor table to maintain a view of the network topology. CiscoWorks is a necessary tool for managing and troubleshooting the network. CDP is used only on internally facing network devices, and is explicitly disabled on all externally facing network device interfaces.
30. Print Spooler — Manages all local and network print queues and controls print jobs. The print spooler is the center of the Windows printing subsystem and controls all printing jobs.
31. Telephony — Provides Telephony Application Programming Interface (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and through the LAN on servers that are also running the service. (IP-Based voice connections are prohibited within the Medicare enclaves.) The telephony service enables applications to act as clients to telephony equipment such as PBXs, telephones, and modems. The service supports the TAPI under which different wire protocols that communicate with telephony equipment can be supported. These protocols are implemented by Telephony Service Providers (TSPs).
32. Terminal Services Licensing — Installs a license server and provides registered client licenses when connecting to a Terminal Server. The Terminal Services License Service is a low-impact service that stores the client licenses that have been issued for a Terminal Server and tracks the licenses that have been issued to client computers or terminals.
33. Distributed Link Tracking Client — Maintains links between NTFS files within a computer or across computers in a network domain.
34. Terminal Services Session Directory — This service provides a multisession environment that allows client devices to access a virtual Windows desktop session and Windows-based programs running on a Windows Server.
35. Upload Manager — The Upload Manager service manages the synchronous and asynchronous file transfers between clients and servers on the network. Driver data is anonymously uploaded from customer machines to Microsoft then used to help users find the drivers required for their systems. The Microsoft Driver Feedback Server asks the client's permission to upload the computer's hardware profile and then search the internet for information about how to obtain the appropriate driver or get support from Microsoft or a third party.
36. Uninterruptible Power Supply — Manages communications with a UPS connected to the computer by a serial port.
37. Virtual Disk Service — The Virtual Disk Service (VDS) provides a single interface for managing block storage virtualization whether done in OS software, Redundant Array of Inexpensive Disks (RAID) storage hardware subsystems, or other virtualization engines.
38. World Wide Web Publishing Service — This service provides HTTP services for applications on the Windows platform. The service contains a process manager and a configuration manager. The process manager controls the processes in which custom applications and simple websites reside. The configuration manager reads the stored system configuration and ensures that

Windows is configured to route HTTP requests to the appropriate application pools or operating system processes.

39. WebClient — The WebClient service allows Win32 applications to access documents on the internet.
40. WinHTTP Web Proxy Auto-Discovery Service — WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration via its implementation of the Web Proxy Auto-Discovery (WPAD) protocol.
41. Portable Media Serial Number — Retrieves the serial number of a portable music player connected to the computer.
42. Messenger — Transmits net send and alerter service messages between clients and servers. Required for clusters.
43. Remote Procedure Call (RPC) Portmapper — An inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction. (UNIX)
44. Network File System (NFS) — Used by all UNIX servers for automated flash archiving and for jumpstart (backup and restore functions).

2.3.4.11 Protection of Information at Rest

This section defines how the organization shall:

- Protect the confidentiality and integrity of sensitive information at rest within the organizational information system or hosted externally.

Protecting the confidentiality of information at rest is about protecting the data or information against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Confidentiality has to do with the privacy of information, including authorizations to view, share, and use it.

Protecting the integrity of information at rest is about the reliability and trustworthiness of data or information.

Information-at-Rest Definition

Information at rest is defined as information (data) that is not in use or is not traveling within the environment.

The recommended protection will vary based upon where the information is resting.

The BlueCross BlueShield of South Carolina enterprise deals in a business process where the majority of information handled is considered sensitive (non-public). The standards are written with this in mind, accepting that the majority of information is sensitive and segregating out the public information is only done in isolated cases.

Mobile Direct Access Storage Device Devices

Mobile Direct Access Storage Device (DASD) relates to information stored on external mobile devices that require attachment to another computing device in order to be utilized. The information on mobile DASD devices must be encrypted.

A Vice President must authorize:

- The use of encrypted and unencrypted mobile DASD devices.
- Whether mobile DASD devices are Read Only or Read and Writing.

Backup Copies

The term *backup copies* (e.g., tapes and platters) refers to information at rest that was copied for later restoration during recovery (e.g., Disaster Recovery) situations. Backup copies must be encrypted to protect information while being moved and while at rest.

Laptops

All laptop hard drives must be encrypted.

Workstation Internal Hard Drives

Only limited amounts of information should be stored on a workstation. The information must be stored within an encrypted container.

Data Center Protected DASD

DASD equipment that is stored within the Data Center that has the required physical access limitations in place does not require any additional protections.

Non-Workstation DASD Devices Outside of the Data Center

These situations should be reviewed for why the devices exist outside of the data center, and if an authorized reason exists, then they should be treated like workstations and are required to be encrypted.

Externally Hosted DASD

Third-Party Service Providers that have our sensitive information at rest at their sites are required to comply with our information-at-rest standards.

Multi-function Devices

The configuration settings for multi-function devices must:

- Clear the data storage upon the completion of a job.
- Enable the encryption of any stored data, if the option is available.

Cloud Services

Third-Party Service Providers and Cloud Service Providers (CSP) that store and process our sensitive information are required to comply with our information-at-rest standards.

The minimal criteria for CSP storage and processing of public and non-public data are as follows:

- Monitoring access and activity
- Alerting and auditing of user activity with data
- Capabilities, such as those listed below, to enforce security policies to proactively secure data and prevent loss:

    - Enforce data protection via encryption
    - Restrict usage (sharing, printing, saving, copying, downloading) based on data sensitivity
    - Enforce use of secure transfer solutions
    - Enforce organization retention policies

Storage of sensitive information must follow the above, and the service must be FedRAMP authorized for Medicare and TRICARE.

For Medicare data, any data considered Medicare Sensitive (including HOST Names, IPs, PII/PHI, Vulnerability and Configuration information), a FedRAMP level of High must be met and LOB approval from CMS must be obtained.

For TRICARE and VA contracts, Controlled Unclassified Information (CUI) (including PII and PHI) requires a FedRAMP level of Moderate. In addition, if available, TRICARE data processing and storage of CUI within the cloud should include DoD IL4 Certification where available. If DoD IL4 Certification is not available, utilization options may be limited.

Data stored within cloud services will be encrypted while at rest. There are two types of encryption keys used to protect data at rest and in transit for the cloud service and resources. Service Managed Keys are keys that are generated, stored and managed entirely by the service providers. They are leveraged to apply encryption to services and resources. Customer Managed Keys are keys that the organization creates, owns and manages. This supports “bring your own key” for applying encryption to services and resources. Customer Managed Keys are stored in an organization-managed key vault/hardware security module (HSM).

The use of Service Managed or Customer Managed keys allows for:

- Generation and use of keys in compliance with FIPS 140-2 requirements
- Ability to encrypt cloud-native data stores
- Enforcement of automated encryption key life cycles
- Auditing key creation, management and use

Service Managed Keys for encryption of cloud services are acceptable unless there is an explicit business or regulatory compliance requirement to use Customer Managed Keys instead for encryption of data at rest and in transit for cloud service and resources.

2.3.5 System and Information Integrity

The following section defines how the organization shall:

- Identify, report, and correct flaws in a timely manner.
- Provide protection from malicious code at appropriate locations.
- Monitor security alerts and advisories, and take appropriate actions in response.

2.3.5.1 Data Integrity Controls

Data integrity controls are in place to protect data from unauthorized modification and to ensure the accuracy, reliability, integrity, and credibility of data throughout its communication. Safeguards are implemented to detect and minimize inadvertent or malicious modification or destruction of data, including system access controls and encryption when residing in non-secure areas.

Although not handled by ICT NH, the BlueCross Data Center utilizes version control software to capture all software changes, identify individuals responsible for making and approving the change, maintain prior versions, identify reasons for the changes, prevent conflicting changes to the software, ensure that the source and object modules correspond, and enforce software change control procedures.

Transmission and storage of data of sensitive information may only be stored on hard disks as long as the security access control devices (hardware/software) approved by the CMS Business Partner:

- Have been installed.
- Are receiving regularly scheduled maintenance, including upgrades.
- Are being used.

Examples of access control devices are:

- Password security
- Audit trails/logs
- Encryption or guided media
- Virus protection
- Data overwriting capabilities

2.3.6 Access and Security

2.3.6.1 Intrusion Monitoring System

Cybersecurity Operations (SecOps) at BlueCross BlueShield of South Carolina (BlueCross) uses Intrusion Monitoring Systems in order to maintain a secure and stable network environment.

SecOps has in place numerous monitoring appliances at strategic locations to monitor the network for malicious activity. Event correlation technologies are also leveraged to help identify real-time attack vectors and alert appropriate teams based on preset triggers. The monitoring logs are reviewed and reports are distributed to the applicable groups for evaluation. Monitoring systems are updated regularly with signatures released by vendors to ensure the highest level of protection is provided.

2.3.6.2 Internet Firewall

BlueCross has implemented next-generation firewalls to provide comprehensive network security for perimeter connections. The perimeter firewalls have the capability to track all communication activities for network and application-level protection.

BlueCross uses these firewalls to protect the network from unauthorized access or malicious activities. They also provide VPN connectivity across un-trusted networks. The firewalls verify the identity of users and permit or deny (inbound or outbound or both) access based on preset security policies.

Changes to firewall policies must be requested using the "Firewall Access Request" form located on the TSC Self-Service.

2.3.6.3 Firewall Rule Review

The SecOps team is responsible for actively monitoring the firewall logs on a daily basis to detect any anomalies.

All firewall rules are reviewed prior to deployment by SecOps as part of the Deployment Management Methodology and Service Request tickets.

In addition, an annual review of all firewall rules is completed by SecOps. Any identified, unacceptable firewall rules are sent to the Network Compliance team for remediation or risk documentation.

2.3.6.4 Vulnerability Scans

In order to maintain a secure and stable network environment, Information Communication Technology (ICT) has been directed to scan all Network Services assets. Scan frequency will be governed by contractual requirements with each line of business. ICT uses state-of-the-art scanning tools to identify security issues. Assessments of the scan results allow ICT to make recommendations for maintaining, patching and upgrading the network assets as deemed necessary. The scan results are reviewed, and reports are distributed to the responsible groups for remediation. Remediation deliverables are regulated by contractual and regulatory requirements.

2.3.6.5 CISCO Secure ACS (TACACS)

We use Cisco Secure ACS to control access to the Cisco network devices.

Cisco Secure ACS provides Authentication, Authorization, And Accounting (AAA—pronounced "triple A") services to network devices that function as AAA clients, such as a network access server, PIX Firewall, or router. The AAA client represents any such device that provides AAA client functionality and uses one of the AAA protocols supported by Cisco Secure ACS.

Cisco Secure ACS centralizes access control and accounting, in addition to router and switch access management. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change privilege levels for entire groups of users.

2.3.6.6 SecurID

RSA SecurID is the corporate standard for remote access authentication at BlueCross due to its two-factor user authentication properties. The RSA SecurID solution uses a token that generates a single-use token code that changes every 60 seconds. The authentication server (RSA ACE/Server) protects the network with this dynamic code. Each RSA SecurID token is unique, and it is impossible to predict the value of a future token code by recording prior token codes since it generates a pseudo-random token

code. When a token code is supplied together with a PIN, there is a high degree of certainty that the person is the valid user in possession of the RSA SecurID authenticator.

In a two-factor authentication session, the user is required to enter a RSA user name and, in lieu of a password, a PIN number plus the current token code from his or her RSA SecurID authentication device. The agent transmits the information to the RSA ACE/Server software, which approves access when the information is validated.

2.3.6.7 Cloud Network Access

Due to cloud services' implicit broad network access characteristic, it's important to ensure that direct public internet access to resources deployed in the cloud are restricted unless explicitly required as a part of the solution and the risk is minimal and acceptable (e.g., public web applications).

Access to cloud compute will be allowed via secure connection through controlled access points only such as bastion hosts or equivalent cloud service (e.g., AWS System Manager).

Network security groups, access control lists or similar solutions must be used to restrict traffic flow to and from cloud compute resources. And in all cases, an application gateway or a web application firewall is required to monitor and restrict traffic.

In cases where there needs to be connectivity established between a Cloud Service Provider (CSP) and an on-premises system for integration purposes, a private connection will be used such as AWS Direct Connect, Azure ExpressRoute or Site-to-Site VPN.

Workloads within the cloud will be restricted to an established private network. In cases where there is a need to expose resources outside of the private network, local, service-based firewalls will be used to restrict access to the resource based on least privilege. Traffic between workloads in the same virtual subnet will be restricted using a cloud firewall (or security group) policy.

2.3.7 Secure FTP – Security Option for the FTP Clients

Secure FTP is used on BlueCross BlueShield of South Carolina's (BlueCross') Enterprise Server. Authentication is established using the Enterprise Server FTP security mechanism. The FTP security mechanism begins with a client telling the Enterprise Server what security mechanism it wants to use with the AUTH command. The Enterprise Server accepts this mechanism, rejects this mechanism, or, in the case of a server (which does not implement the security extensions), rejects the command completely. The Enterprise Server's reply indicates if the client must respond with additional data for the security mechanism to interpret.

Once a security association is established, authentication (which is part of this association) may be used in addition to the standard user ID/password exchange for authorizing a user to connect to the Enterprise Server. A user ID specified by the USER command is always required to verify the identity to be used on the Enterprise Server for Secure FTP.

NOTE A request for a Key/Certificate on the Client side must be requested from BlueCross RACF ADMIN for approval and usage to the BlueCross Enterprise Server. A Key/Certificate is used for identification of the Client and encryption of data to and from the BlueCross Enterprise Server.

2.4 Security Systems

The Security Triad (CIA)

The technologies outlined in this chapter are used to enforce the BlueCross BlueShield of South Carolina (BlueCross) security triad of Confidentiality, Integrity and Access (CIA) of information:

- Confidentiality — The property of systems and data to be accessible only to those properly authorized to have access.
- Integrity — The property of systems and data to be correct and true, and to ensure against data loss and or corruption.
- Availability — The property of systems and data to be operable and committable whenever the mission calls for it.

Security technologies are installed on Hosts or in security enclaves as required under guidelines not outlined in this chapter.

2.4.1 Authentication, Authorization and Accounting

We deploy Authentication, Authorization and Accounting (AAA) products to address integrity and confidentially through the products' performance of any or all of the following functions within the infrastructure:

- Authentication is the establishment of digital identity. Each authentication can be made up of from one to three of these factors: something you know, something you have and something you are. We use two-factor authentications at BlueCross.
- Authorization is the assignment of privileges to a digital identity.
- Accounting refers to the tracking of actions taken by the digital identity.

The approved AAA products are listed below (Table 2-2).

Approved AAA Products

Product	Description
Cisco Identity Services Engine (ISE)	Cisco ISE implements Network Access Control (NAC), which is an authentication system that ensures that a workstation connecting to the network is authorized and meets certain criteria for security before a connection is allowed. In most NAC systems, a non-compliant workstation is sent to a remediation LAN to be brought up to standard, then it is authorized. Additionally, Cisco ISE provides wired and wireless authentication through 802.1x and network device administration through TACACS+ and RADIUS.
Directory Smart	This is an implementation of Lightweight Directory Access Protocol (LDAP) used as an application directory in our customer/outward facing Demilitarized Zone (DMZ).

Approved AAA Products

Product	Description
IBM DataPower	Web Services
IBM Managed File Transfer (MFT) Suite — IBM Sterling B2B Integrator	IBM® Sterling B2B Integrator helps integrate complex B2B and EDI processes across partner communities in a single gateway. It provides a flexible platform, available on premises or through hybrid cloud, that supports data transformation and most communication protocols.
Lightweight Directory Access Protocol (LDAP)	LDAP is a protocol, which is an industry standard, and only provides the mechanisms required for authentication. Many vendors provide LDAP implementations, and we have more than one here at BlueCross.
RSA SecurID	RSA SecurID is a product that provides two-factor authentication. Two-factor authentication is required in various places for compliance and security. Basically, RSA SecurID checks a code sent to the system from a user. The code is presented on a token, and that combined with the PIN presents a one-time password only that user can know.
Specops Password Policy	This software is a Microsoft Active Directory add-in that allows system administrators to require more complex passwords than can be required in Active Directory natively.
Oracle Directory Server (SunOne)	Sun Microsystems implementation of LDAP
Oracle Identity Management	A Sun Microsystems-developed identity management system, now owned by Oracle, which allows identities from several systems to be federated.
UserLock	UserLock allows system administrators to limit the number of times an administrator or user is logged into an Active Directory domain. It is an AD add-in.

Table 2-2 Approved AAA Products

2.4.2 Encryption

All compliance boundaries within BlueCross BlueShield of South Carolina (BlueCross) enclave must use encryption technologies that meet or exceed Federal Information Processing Standard (FIPS)-validated cryptography to protect the confidentiality, integrity and availability of sensitive information stored and in transit. Continuous monitoring of this requirement must be supported.

Removable media and mobile devices connected to or in use for all compliance boundaries in relation to BlueCross data will employ full device or container encryption.

2.4.3 Endpoint Protection/Malware Protection

Communication channels and data storage points are open to attack by malware and must be protected. Malware is the term, which comes from the term *malicious software*, for all types of damaging software such as viruses, worms, Trojan horses and spyware. The legal term for this software is *computer contaminate*. Malware is designed to breach computer systems without the system owner's knowledge. The intent is to damage, disrupt or profit. Protection software is installed at potential technical attack vectors such as email, file shares, portal sites, websites, and portable media and onto the kernel of endpoint operating systems. This software detects and prevents the installation and spread of malicious software (virus and malware), probes and scans by unauthorized sources, and users deemed to be injurious to the system. Protection software can be loaded on to an individual Host server or on to a workstation. Endpoint protection enforces all elements of the security triad.

As a general standard, all files on all affected Hosts will be protected. An exception process exists, and exceptions will be on file for any excluded files. Exceptions will be managed per application or per Host.

The approved endpoint protection products are (Table 2-3):

Approved Endpoint Protection Products

Product	Description
McAfee ePolicy Orchestrator	ePolicy Orchestrator (ePO) is the McAfee console used to deliver, update and configure all McAfee products from a single location. This allows a consistent set of rules to be applied across thousands of end points.
McAfee Security for Microsoft Exchange	McAfee Security for Microsoft Exchange (MSME) installs on Microsoft Exchange Mailbox servers. It scans mailboxes and email in transit at the hubs and SMTP entry points for viruses and SPAM. MSME is managed by ePO. This software works by signatures, which are frequently updated to look for specific file types and characteristics.
McAfee Security for Microsoft Sharepoint	McAfee Security for Microsoft SharePoint (MSMS) is a software package loaded on Microsoft SharePoint Portal Servers. MSMS protects the portal from virus uploads, and it scans existing content for the presence of malware in several forms. The product is managed and updated by ePO.
McAfee VirusScan Enterprise for Storage	This product is used for malware protection for NetApp vFilers on Network Attached Storage (NAS) devices.
McAfee VirusScan Command Line Scanner	VirusScan Command Line Scanner is used in the Non-Host UNIX environment for malware protection. The product is updated frequently with signatures, which are used in the comparison of files to detect viruses. VirusScan Command Line Scanner allows for an on-demand scan where all or a subset of the files in a Non-Host Unix environment are scanned.
McAfee VirusScan Enterprise	VirusScan Enterprise (VSE) is a product, which takes the

Approved Endpoint Protection Products

Product	Description
	form of installed software, managed by ePO. VSE is updated frequently with signatures, which are used in the comparison of files on access to detect viruses. VSE also allows for an on-demand scan where all or a subset of the files on a Windows Host are scanned.
Proofpoint	Proofpoint inspects email traffic as it flows to and from the email environment for forbidden and sensitive data.

Table 2-3 Approved Endpoint Protection Products

2.4.4 Enterprise Security Event Logging and Management

A Security Information and Event Management (SIEM) system is the glue of a security system, used to enforce all elements of the security triad. It consolidates, filters and normalizes data from disparate devices across the enterprise network to provide a centralized, holistic view of the security status of all relevant IT systems. The SIEM system gathers the data produced by other security systems, correlates the input, and helps integrate security into existing management processes and workflows.

Being able to correlate data from many different collection points and to add logic is vital to knowing when and how to act. All components of the network and systems infrastructure generate logs; who accessed the system, what they did, and when are recorded. These logs must be pulled together in a common format, normalized and aggregated to create a whole. The aggregated logs give a view of the organization's activities, which may be used for many security purposes including forensics and analysis.

The approved log and security event management products are (Table 2-4):

Approved Log and Security Event Management Products

Product	Description
ArcSight Connectors	ArcSight Connectors allow individual devices to be connected to the larger log collection and aggregation system. These are basically software-based parsers that take one log format and change it to a standard format.
Amazon Web Services (AWS) Cloud Trail	AWS Cloud Trail continuously monitors and retains account activity related to actions across AWS infrastructure. This service integrates with Exabeam for log aggregation.
Azure Log Analytics	Within Azure Monitor, Azure Log Analytics are unique workspace environments for the collection of audit and security log data from Azure services. This service integrates with Exabeam for log aggregation.
Exabeam AA/IR	Exabeam AA/IR is part of the Exabeam system where alerts are generated, and events that require some sort of action are

Approved Log and Security Event Management Products

Product	Description
	examined.
Exabeam Data Lake	Exabeam Data Lake devices gather and maintain logs from individual devices.
Network Time Protocol (NTP)	NTP is an internet standard protocol that provides a mechanism for disseminating correct time to all devices. At BlueCross, two external sources are referenced, then several devices are used as distribution points to ensure that time is always correct and synchronized.
SYSLOG	SYSLOG is an internet standard protocol that provides a default format and way to make and move system event log data.

Table 2-4 Approved Log and Security Event Management Products

2.4.5 Firewalls

A firewall is a system or device designed to prevent unauthorized electronic access to networks or systems. It enforces separation of security domains. We employ packet filtering firewalls which inspect the source and destination of each network packet, and drop those which are not explicitly allowed. Firewalls ensure confidentiality and integrity of the systems they protect.

The approved firewall products are (Table 2-5):

Approved Firewall Products

Product	Description
Checkpoint Firewall	Checkpoint firewalls are used in the internet facing role.
Cisco ASA-5500 Adaptive Security Appliance (ASA)	Cisco firewall service modules in ASA appliances are used to separate security enclaves within the BlueCross network.
Cisco Private Internet Exchange (PIX)	Cisco PIX is used to separate security enclaves within the BlueCross network. This is being replaced with ASA appliances.
Juniper NetScreen (NS-500ES-FEI-AC)	Advanced firewall system which is used in the EDC. This technology is also used in several, three tier environments so as to provide defense in depth by mixing firewalls between layers.

Table 2-5 Approved Firewall Products

2.4.6 Internet Traffic Filter

Internet Traffic Filter systems include hardware and software which allows or denies access to specific types of information to or from the internet. These systems enforce confidentiality because they filter undesired aspects of internet-based information from entering the network.

The approved internet filter products are (Table 2-6):

Approved Internet Filter Products

Product	Description
Palo Alto URL Filtering Web Security	This device performs internet site filtering for the corporation. All websites visited are checked against whitelists and blacklists, and also checked for category. Any website that meets certain criteria is blocked. This does not apply to server Out-of-Band Management (OOBM) traffic.
Blue Coat	This device performs internet site filtering for internet traffic originating from within the Out of Band Management (OOBM) server network.

Table 2-6 Approved Internet Filter Products

2.4.7 Intrusion Detection (Network and Host Based)

Intrusion Detection systems look for patterns to identify possible attacks. Network Intrusion Detection Systems (NIDS) detect malicious activity on a network directed towards individual components of the infrastructure. NIDS inspect incoming traffic for malicious attacks, and also check outgoing network traffic for data leakage. Intrusion Prevention Systems (IPS) are a special class of NIDS that may be deployed to actually stop malicious activity or data leakage when detected.

NIDS enforce all elements of the security triad. Host Intrusion Detection System (HIDS) is installed on a server or endpoint to look for malicious activity at the operating system level.

There are two types of intrusion detection at BlueCross: Host-Based Intrusion Detection and Network-Based Intrusion Detection. Intrusion detection systems may be signature based or behaviorally based.

There is a definition for HIDS that must be followed when selecting products. The product must:

- Monitor logs for anomalies, which may detect malicious behaviors coming from the Host system or coming to the Host system.
- Monitor key system files for changes (executable and configuration files).
- Alert the appropriate Enterprise Architect when an incident has been detected.
- Alert, report and log through the SIEM system.
- Have other settings as deemed necessary to meet or exceed our compliance and regulatory requirements.

The approved intrusion detection products are (Table 2-7):

Approved Intrusion Detection Products

Product	Description
Advanced Intrusion Detection Environment (AIDE)	The AIDE was initially developed as a free replacement for Tripwire licensed under the GPL. The purpose is to monitor system files for unauthorized changes, thereby allowing systems administrators to ensure the integrity of their systems.
Host Intrusion Prevention for Server (HIPS)	HIPS is software installed on Medicare and PGBA Hosts, which looks for out-of-the-ordinary behavior on the Host. This type of system is called “behavior based” because it baselines the behavior of the system and looks for changes to that behavior. HIPS may be run in a learn mode, during which period the system activity is profiled. It is then placed in block mode, where unlearned behavior is stopped.
Cisco Intrusion Detection System	Cisco Intrusion Detection Systems are used throughout our network and in internet- and customer-facing DMZs.

Table 2-7 Approved Intrusion Detection Products

2.4.8 Public Key Infrastructure

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It contains your name, a serial number, expiration dates, and a copy of the certificate holder's public key. The key is used for encrypting messages and digital signatures. The certificate also carries the digital signature of the certificate-issuing authority so a recipient can verify that the certificate is real.

This type of system enforces integrity and confidentiality.

The approved PKI products are (Table 2-8):

Approved Intrusion Detection Products

Product	Description
Comodo Instant SSL Certificates	Comodo is a vendor of SSL certificates and one of the vendors allowed at BlueCross.
Oracle OpenSSO Enterprise	The main purpose of the OpenSSO Enterprise product is to provide an easy and powerful way to enable using Single Sign-On with many legacy software products, which do not support this feature natively. User identification relies on x509 certificates, which can be provided through a third party CA system.

Approved Intrusion Detection Products

Product	Description
Verisign SSL Certificates	Verisign is a vendor of SSL certificates and one of the vendors allowed at BlueCross.

Table 2-8 Approved Intrusion Detection Products

2.4.9 Remediation, Patch and Configuration Management

Remediation, Patch and Configuration systems track the physical and operational characteristics of hardware and software used in the infrastructure. These systems:

- Affect changes to ensure that the systems are compliant with applicable governance.
- Help to minimize change impact.
- Facilitate system compliance to enforceable standards.
- Address availability and integrity.

Under the shared responsibility model, BlueCross BlueShield of South Carolina (BlueCross) is responsible for operating system and application Remediation, Patch and Configuration management for all Infrastructure as a Service (IaaS) deployed to the cloud. The existing Service Level Agreements (SLAs) for patching systems and applications apply to the cloud.

The approved remediation, patch and configuration products are (Table 2-9):

Approved Remediation, Patch and Configuration Products

Product	Description
AWS Config	AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.
AWS Systems Manager Patch Manager	AWS Systems Manager Patch Manager automates the process of patching managed nodes with both security-related and other types of updates for both Windows and Unix in AWS. This product is used to apply patches for both operating systems and applications.
Azure Policy	Azure Policy evaluates resources in Azure by comparing the properties of those resources to established policy definitions.
Azure Update Management	Azure Update Management is used to manage operating system updates for both Windows and Unix virtual machines in Azure.
Microsoft Windows Update Server	WSUS is used to deliver patches to all servers in all security enclaves. It cannot be used to affect software delivery or

Approved Remediation, Patch and Configuration Products

Product	Description
(WSUS)	configuration. It is only capable of patching, and only on Windows.
Tivoli Endpoint Management (TEM)	TEM is used for vulnerability management in the Non-Host Windows and UNIX environments.
Group Policy Object (GPO)	GPO is used to set and enforce configuration settings on Windows servers.

Table 2-9 Approved Remediation, Patch and Configuration Products

2.4.10 Virtual Private Network

A Virtual Private Network (VPN) is a private network that uses a public network (usually the internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses "virtual" connections routed through the internet from the company's private network to the remote site or employee.

The approved VPN products are (Table 2-10):

Approved VPN Products

Product	Description
Cisco ASA-5500 Series Adaptive Security Appliance	This device allows the addition of several modules which serve a variety of security purposes. VPN is one of the purposes, and is the primary VPN provider for BlueCross.

Table 2-10 Approved VPN Products

2.4.11 Vulnerability Scanners and Management Systems

Vulnerability Scanners determine if there are known deficiencies in the system, which could be used by an attacker to penetrate, deface or deny access to a system.

The approved vulnerability scanning products are provided in the following table (Table 2-11):

Approved Vulnerability Scanning Products

Product	Description
AppDetective	AppDetective is a system that scans databases for common errors, which may constitute vulnerabilities. This scanner is used in all security enclaves and the corporate environment

Approved Vulnerability Scanning Products

Product	Description
	where appropriate.
Fluke Wireless Access Detection Device	This device is used to detect unauthorized WLAN hotspots or wireless activity.
Nessus	Nessus is the network and Host vulnerability scanner used in the Medicare enclave.
Nessus Security Center (SC)	Nessus SC is used to manage scans and workloads on multiple Nessus scanners. It is set up for use inside the Medicare enclave.
Nmap	This is a free, industry-standard network and port scanner. It is used to develop lists of Hosts through discovery, and then the ports open on each Host by performing port sweeps on the Host.

Table 2-11 Approved Vulnerability Scanning Products

2.4.12 Data Loss Protection

Data Loss Protection (DLP) products:

- Detect and prevent the unauthorized use and transmission of confidential information.
- Identify, monitor, and protect:
    - Data in use (e.g., endpoint actions).
    - Data in motion (e.g., network actions).
    - Data at rest (e.g., data storage).
- Employ deep content inspection and contextual security analysis of a transaction (e.g., attributes of originator, data object, medium, timing, recipient/destination, etc.).
- Work within a centralized management framework.

Approved DLP products are listed below in Table 2-12.

Approved Data Loss Protection Products

Product	Description
Proofpoint	Proofpoint inspects email traffic as it flows to and from the email servers for forbidden and sensitive data.

Approved Data Loss Protection Products

Product	Description
McAfee Endpoint DLP	This product is installed on endpoints and is centrally controlled by McAfee ePolicy Orchestrator (ePO) to enforce policies pertaining to the accessibility of Universal Serial Bus (USB) jump drives, display prints and printers. The purpose is to control what data is allowed to move to external drives and devices.
Microsoft Purview Data Loss Prevention (DLP)	This product prevents the unintentional or accidental sharing of sensitive information based on pre-defined policies and classifications.

Table 2-12 Approved Data Loss Protection Products

2.4.13 Cloud Image Management

Hardened images are pre-configured to meet organizational standards, have appropriate configuration settings applied, and have integrated security validation and testing into the image creation process. Only BlueCross hardened images are authorized for deployment to production workloads in the cloud. As with existing platforms, deploying unmanaged images from unauthorized sources into BlueCross-managed cloud environments is not authorized.

Chapter 3 Application Security

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

3.1 RACF Security Coding Procedures

3.1.1 Procedures to Query RACF Security

The *EXEC CICS QUERY SECURITY* command allows an application to query the RACF database to determine if a specific User ID or group has access to a protected resource.

3.1.1.1 Query Security Command

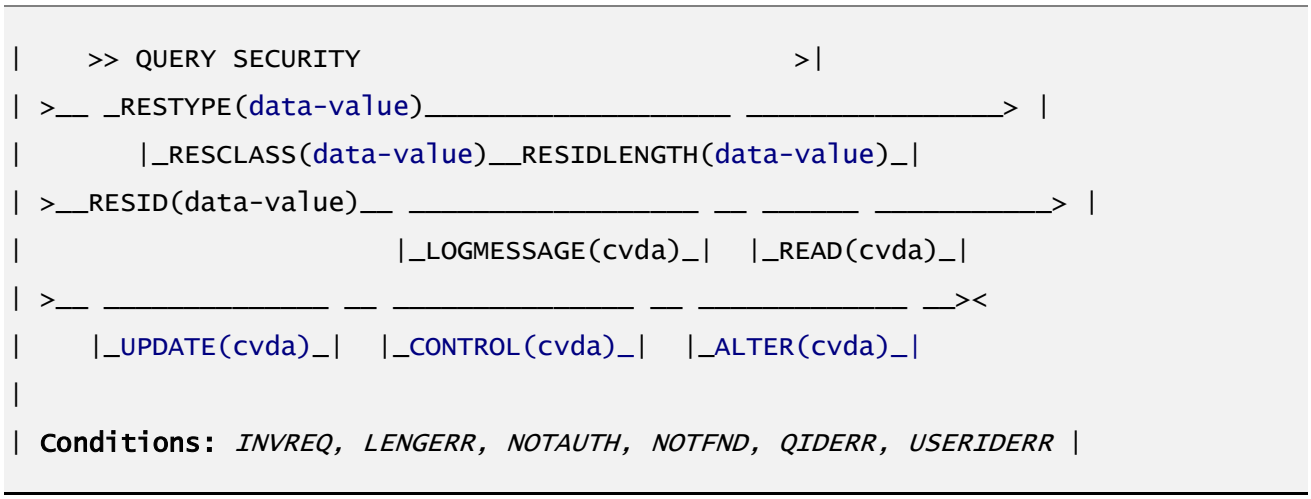
QUERY SECURITY is effective with RACF, and you can use this command to query whether the terminal user has access to resources that are defined to the external security manager. These can be:

- Resources in CICS resource classes
- Resources in user-defined resource classes

The terminal user in this context is the user invoking the transaction that contains the *QUERY SECURITY* command. In response to a *QUERY SECURITY* command, CICS returns information about the terminal user's security authorizations. CICS obtains this information from the external security manager. You can code the application to proceed in different ways depending on the user's permitted accesses. You specify the type of resource that you are querying by the CICS resource type name. For example, if you want to query a user's authorization to access a file, you can specify RESTYPE('FILE'). To identify a particular file within the type, you specify the RESID parameter.

3.1.1.2 Query Security

To *query* the *security* authorization of the user.



Description

QUERY SECURITY allows the application to determine whether the user has access to resources defined in RACF. These resources can be:

- In CICS resource classes.
- In user-defined resource classes.

If USERID is not specified, the user to be queried is the user that invokes the transaction issuing the Query Security command.

Alternatively, the application can query the security authorization of a different user that is specified in the USERID option.

For more information on the use of the Query Security command, see the CICS RACF Security Guide.

Options

ALTER(cvda) – Query whether the user has ALTER authority for the named resource. The cvda values returned by CICS are ALTERABLE and NOTALTERABLE.

CONTROL(cvda) – Query whether the user has CONTROL authority for the named resource. The cvda values returned by CICS are CTRLABLE and NOTCTRLABLE.

LOGMESSAGE(cvda) – Inhibit security violation messages. The values passed to CICS are LOG (the default value) or, to inhibit messages, NOLOG.

READ(cvda) – Query whether the user has READ authority command for the named resource. The cvda values returned by CICS are READABLE and NOTREADABLE. READ access authority usually permits nondestructive use of a resource as, for example, in the case of READ and INQUIRE commands.

RESCLASS(data-value) – Specifies an 8-character field identifying the name of a valid resource class, which could be non-CICS, in the ESM. The class name identified by RESCLASS is treated literally with no translation. If the ESM is RACF, the class can be CICS-supplied or user-defined. RESCLASS enables you to define more narrowly the authorization to be queried; for example, you can query at the record or field level.

RESID(data-value) – Specifies the name of the CICS or user-defined resource you want to query the users access to. The value is a character string (1-12 characters for a CICS resource, and 1-246 characters for a user-defined resource, unless you are using the COBOL3 translator option in which case the maximum length is 160 characters. Note that the actual resource checked depends on whether RESCLASS or RESTYPE is specified in the command and whether prefixing is active (SECPRFX=YES or SECPRFX=prefix specified as a system initialization parameter).

If RESCLASS is specified, the resource checked is always the actual RESID data-value, whether or not prefixing is on or off. If RESTYPE is specified and prefixing is not active (SECPRFX=NO), the resource checked is the specified RESID value. Otherwise the resource checked is the RESID value prefixed with either the CICS region userid (if SECPRFX=YES), or another prefix (if SECPRFX=prefix)

RESIDLENGTH(data-value) – Specifies the length, as a fullword binary, of the resource identifier in RESID. You only use this parameter when specifying the RESCLASS option.

RESTYPE(data-value) – Specifies the type of resource (1-12 characters) you want to query the user's access to. The responses returned by the command reflect the results that would be obtained if an actual attempt was made to access the specified CICS resource. The value you specify for RESTYPE must be one of the following resource types (Table 3-1):

Query Security RESTYPE Values

RESTYPE Value	Xname Parameter
ATOMSERVICE	XRES
BUNDLE	XRES
DB2ENTRY	XDB2
DOCTEMPLATE	XRES
EPADAPTER	XRES
EPADAPTERSET	XRES
EVENTBINDING	XRES
FILE	XFCT
JOURNALNAME	XJCT
JOURNALNUM[1]	XJCT
JVMSERVER	XRES
PROGRAM	XPPT
PSB	XPSB
SPCOMMAND[2]	XCMD
TDQUEUE	XDCT
TRANSACTION	XPCT
TRANSATTACH	XTRAN
TSQUEUE	XTST
TSQNAME	XTST
XMLTRANSFORM	XRES

Notes:

[1] Supported for compatibility with earlier releases.
[2] SPCOMMAND is a resource type that you can use to specify a RESID for a command.

Table 3-1 Query Security RESTYPE Values

The **XHFS** system initialization parameter controls resource security for zFS files and does not have a corresponding RESTYPE value on the **QUERY SECURITY** command. Access controls for zFS files follow the system of permissions used by z/OS UNIX System Services, so they operate in a different way.

With dynamic transaction routing, you do not have to install transaction definitions in terminal owning regions. A *QUERY SECURITY* command with a RESTYPE of TRANSATTACH returns the NOTFND condition if the transaction is not installed. Application developers must be aware that the transaction might be routed dynamically.

If you issue **QUERY SECURITY RESTYPE(TRANSATTACH) RESID(tranid) Read(cvda)**, this command returns the CVDA value of READABLE if the user has READ authority for the resource with the name *tranid*, but NOTREADABLE if the user has only EXECUTE authority. Therefore, applications that use **QUERY SECURITY RESTYPE(TRANSATTACH)** to build a menu of available transactions will not work if EXECUTE authority is used.

UPDATE(*cvda)* – Query whether the user has UPDATE authority for the named resource. The CVDA values returned by CICS are UPDATEABLE and NOTUPDATEABLE. UPDATE access authority usually permits destructive use of a resource as, for example, in the case of WRITE, DELETE or UPDATE.

USERID(*data-value)* – Specifies the 8-character user ID of the user whose access to the specified resources is queried. The user who invokes the transaction issuing the **QUERY SECURITY** command must have necessary authority to query whether another user as specified in USERID has access to the specified resource. CICS performs a surrogate user check to verify whether the user invoking the transaction is authorized to the user specified in USERID. If the surrogate user check fails, CICS returns a NOTAUTH condition.

Conditions

16 INVREQ

RESP2 values:

7 The cvda value is not valid for the LOGMESSAGE.

9 The RESID is invalid or filled with blanks.

10 The external security manager (ESM) is inactive or not present.

Default action: terminate the task abnormally.

22 LENGERR

RESP2 values:

6 RESIDLENGTH value is not valid, that is, not in the range 1 through 246.

Default action: terminate the task abnormally.

70 NOTAUTH

RESP2 values:

102 The surrogate user security check on the specified USERID fails.

The security access capabilities of the transaction that issued the command do not allow the command to be performed with the value specified in the USERID option.

The security access capabilities of the transaction have been established by the external security manager according to the user security, and whether link security or the execution diagnostic facility (EDF) has been in use.

Default action: terminate the task abnormally.

13 NOTFND

RESP2 values:

1 The RESID is not valid.
2 The RESTYPE is not valid.
3 The RESID value for RESTYPE (SPCOMMAND) is not valid.
5 The RESCLASS is not defined to the external security manager (ESM).
8 The resource is not protected. This is only returned when *QUERY SECURITY* is used with the RESCLASS option (and never occurs with RESTYPE).

Possible causes include:

- RESCLASS not active.
- No profile found.
- RACF not active.
- Default action: terminate the task abnormally.

44 QIDERR

RESP2 values:

1 An indirect queue name associated with the given RESID is not found.
Default action: terminate the task abnormally.

69 USERIDERR

RESP2 values:

11 The specified USERID is not known to the external security manager.
12 The specified USERID is revoked.

3.1.2 Security Application Coding Examples

3.1.2.1 AppMaster Builder (AMB) Coding Example

```
SYM1    % &TP-RETRY      = 0                                                  00010000
         % &TP-USER-LEN   = 1200                                               00020000
 /*      ************************************************************         00030000
 /*      *             INTER-PLAN TELEPROCESSING SERVICES  (ITS)      *       00040001
 /*      *                                                            *       00050001
 /*      *  MODULE:       ITSSD916                                    *       00060016
 /*      *  NAME:         ITSS CICS SECURITY MODULE                   *       00070016
 /*      *                                                            *       00080001
 /*      *  APPLICATION:  ITSSA002                                    *       00090016
 /*      *  TYPE:         CICS AMB                                    *       00100016
 /*      *  FUNCTION:    LINK TO THIS MODULE TO INTERROGATE A USER'S   *       00110001
 /*      *               SECURITY AUTHORIZATION; FIRST USE IS FOR      *       00120001
 /*      *               TRANSACTION ID AUTHORIZATION CHECKING; MAY    *       00130016
 /*      *               BE USED FOR OTHER SECURITY CHECKS IN FUTURE   *       00140001
 /*      *                                                            *       00150001
 /*      *  MODIFICATION                                              *       00160001
 /*      *                                                            *       00170001
 /*      *  DATE: 02/29/04 01.0 INITIAL RELEASE                       *       00180001
 /*      *                                                            *       00190001
 /*      ************************************************************         00200001
                                                                               00200117
 /*      ************************************************************         00201017
 /*      *               INDICATOR SETUPS FOR ITSSD916                *       00202017
 /*      *                                                            *       00203017
 /*      * CM-SEC-WRITE-VIOL-TO-LOG-SW                                *       00204017
```

```
/*      *        SET TO 'Y' TO WRITE TO LOG IF SECURITY ERROR          00205017
/*      *        SET TO 'N' IF YOU DO NOT WANT TO WRITE TO LOG         00206017
/*      *          *** USE 'N' FOR TESTING IF POSSIBLE ***             00207017
/*      *                                                              00209017
/*      * CM-SEC-RESOURCE-CLAS-VALUE                                   00209117
/*      *        '$CICSFLD' IS USED FOR COLLECTION ID RACF CHK         00209217
/*      *        '????????' OTHER VALUES MAY BE USED IN FUTURE         00209317
/*      *        '????????' OTHER VALUES MAY BE USED IN FUTURE         00209417
/*      *                                                              00209517
/*      * CM-SEC-RESOURCE-LENGTH                                       00209617
/*      *         +0008      IS USED FOR COLLID RACF CHECK             00209717
/*      *         +????      OTHERS USED IN FUTURE (MAY                00209817
/*      *                    REQUIRE CODE CHANGE)                      00209917
/*      *                                                              00210017
/*      ****************************************************************00210117
                                                                        00210217
/*      ****************************************************************00210317
/*      *                LINKAGE DOCUMENTATION                         00210417
/*      *                                                              00210517
/*      * CM-SEC-RESOURCE-VALUE                                         00210617
/*      *        'UGTM' IS AN EXAMPLE OF A TRANSACTION ID              00210717
/*      *               USED WITH $CICSFLD FOR COLLID                  00210817
/*      *               RACF SECURITY CHECK                            00210917
/*      *        '????' OTHER RESOURCE VALUES MAY BE                   00211017
/*      *               USED IN FUTURE (MAY NEED CODE CHG)             00211117
/*      *                                                              00211217
/*      * CM-SEC-EXIT-NAME           SET TO SPACES FOR NOW             00211317
/*      *                                                              00211417
/*      * CM-SEC-RETURN-CODE                                           00211517
/*      * CM-SEC-RETURN-CVDA-AREA                                      00211617
/*      * CM-SEC-RETURN-MSG-SHORT                                      00211717
/*      * CM-SEC-RETURN-MSG-LONG                                       00211817
/*      *                                                              00211917
/*      *   RETURN CODE EXPLANATIONS                                   00212017
/*      *                                                              00212117
/*      *    ** NOTE: SOME OF THESE PERTAIN TO THE COLLID RACF         00212217
/*      *    ** CHECK; MAY BE USED DIFFERENTLY FOR OTHER RESOURCE      00212317
/*      *    ** CLASSES USED IN FUTURE                                 00212417
/*      *                                                              00212517
/*      *  +0000  GOOD CALL   FOR COLL ID CHK, THE COLLID DOES EXIS    00212617
/*      *                   AND THE USER IS AUTHORIZED FOR IT)         00212717
/*      *                                                              00212817
/*      *          THE 3500 SERIES IS RESERVED FOR WARNING MESSAGES    00212917
/*      *                                                              00213017
/*      *  +3502  NOTREADABLE (FOR COLLID CHK, THE COLLID EXISTS BUT   00213117
/*      *                      THE USER IS NOT AUTHORIZED FOR IT)      00213217
/*      *  +3503  NOTFND      (FOR COLLID CHK, USER WAS NOT            00213317
/*      *                 AUTHORIZED FOR THAT COLLECTION ID, AND THE   00213517
/*      *                 COLLID PROBABLY DOESN'T EXIST YET)           00213617
/*      * +3599  UNKNOWN     (NOT ABLE TO DETERMINE USERS AUTHORITY     00213717
/*      *                     FOR THAT COLLECTION ID)                  00213817
/*      *                                                              00213917
/*      *          THE 3600 SERIES IS RESERVED FOR SEVERE MESSAGES     00214017
/*      *                                                              00214117
/*      * +3601  INVREQ   CICS HANDLE CONDITION                        00214217
/*      * +3602  LENGERR  CICS HANDLE CONDITION - PROBABLY A BAD       00214317
/*      *                   RESOURCE LENGTH IN THE LINKAGE AREA        00214417
/*      * +3603  QIDERR   CICS HANDLE CONDITION                        00214517
/*      * +3604  BADLOGSW (CALLING PROGRAM MUST SET LOG SWITCH TO      00214617
/*      *                       'Y' OR 'N')                            00214717
/*      *                       ***************                        00214817
/*      ***                     *LENGTH = +106*                        00214917
```

```
/*                              ***************                          00215017
                                                                         00216017
WS01    RESCLAS-VALUE               PIC X(08)       VALUE SPACES.       00220000
WS01    CVDA-AREA                   PIC S9(8)  COMP VALUE 0.            00230000
WS01    CVDA-LOG                    PIC S9(8)  COMP VALUE 0.            00240000
WS01    CVDA-NOLOG                  PIC S9(8)  COMP VALUE 0.            00250000
WS01    RESOURCE-VALUE              PIC  X(8)       VALUE SPACES.       00260000
WS01    RESOURCE-LENGTH             PIC S9(8)  COMP VALUE 0.            00270000
                                                                        00280000
LK01    COPY CMRACF01.                                                  00290013
                                                                        00390000
PROC    USING WS-CA-PASSING-AREA                                        00400013
       PERFORM 1000-INITIALIZATION                                      00402000
       IF CM-SEC-RETURN-CODE = +3699                                    00403000
       PERFORM 2000-MAINLINE                                            00404000
       ESCAPE                                                           00406000
                                                                        00407000
PARA    1000-INITIALIZATION                                             00410000
                                                                        00410114
        MOVE 'N'                TO CM-SEC-WRITE-VIOL-TO-LOG-SW          00411014
        MOVE +0008              TO CM-SEC-RESOURCE-LENGTH               00412014
        MOVE SPACES             TO CM-SEC-EXIT-NAME                     00413014
                                                                        00414014
        CM-SEC-RETURN-CODE      = +3699                                 00420000
        CM-SEC-RETURN-MSG-SHORT = 'SEC +3699 BAD INITIAL'               00430000
        CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3699:  '                00440000
        ... && 'ERROR DURING INITIALIZATION'                            00450003
                                                                        00460000
        CVDA-LOG                = DFHVALUE(LOG)                         00470014
        CVDA-NOLOG              = DFHVALUE(NOLOG)                       00480014
                                                                        00490000
        RESCLAS-VALUE           = CM-SEC-RESOURCE-CLAS-VALUE            00500014
        RESOURCE-VALUE          = CM-SEC-RESOURCE-VALUE                 00510014
        RESOURCE-LENGTH         = CM-SEC-RESOURCE-LENGTH                00520014
                                                                        00530000
        IF  CM-SEC-WRITE-VIOL-TO-LOG-SW = 'Y' OR                        00540000
        ... CM-SEC-WRITE-VIOL-TO-LOG-SW = 'N'                           00550000
            CONTINUE                                                    00560000
        ELSE                                                            00570000
            CM-SEC-RETURN-CODE      = +3604                             00580000
            CM-SEC-RETURN-MSG-SHORT = 'SEC +3604 INV LOG SW'            00590000
            CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3604:  '            00600000
            ... && 'LINKAGE LOG SWITCH NOT Y OR NO'                     00610003
                                                                        00620000
PARA    2000-MAINLINE                                                   00630004
        CM-SEC-RETURN-CODE      = +3599                                 00640000
        CM-SEC-RETURN-MSG-SHORT = 'SEC +3599 ACCESS UNKN'               00650000
        CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3599:  '                00660000
        ... && 'NO USER ACCESS - REASON UNKNOWN '                       00670003
                                                                        00680000
        CICS HANDLE CONDITION                                           00681002
        ...  INVREQ(2100-INVREQ-CONDITION)                              00682002
        ...  LENGERR(2200-LENGERR-CONDITION)                            00683002
        ...  NOTFND(2300-NOTFND-CONDITION)                              00684002
          ...  QIDERR(2400-QIDERR-CONDITION)                           00685002
                                                                        00686002
        IF CM-SEC-WRITE-VIOL-TO-LOG-SW = 'Y'                            00690000
           CICS QUERY SECURITY                                          00700000
           ...  RESCLASS(RESCLAS-VALUE)                                00710000
           ...  RESID(RESOURCE-VALUE)                                  00720000
           ...  RESIDLENGTH(RESOURCE-LENGTH)                           00730000
           ...  READ(CVDA-AREA)                                        00740000
```

```
            ...  LOGMESSAGE(CVDA-LOG)                                    00750000
         ELSE                                                            00760000
            CICS QUERY SECURITY                                          00770000
            ...  RESCLASS(RESCLAS-VALUE)                                 00780000
            ...  RESID(RESOURCE-VALUE)                                   00790000
            ...  RESIDLENGTH(RESOURCE-LENGTH)                            00800000
            ...  READ(CVDA-AREA)                                         00810000
            ...  LOGMESSAGE(CVDA-NOLOG)                                  00820000
                                                                         00830000
         CM-SEC-RETURN-CVDA-AREA  = CVDA-AREA                            00840004
                                                                         00850000
         EVALUATE TRUE                                                   00860000
            WHEN CVDA-AREA = DFHVALUE(READABLE)                          00870000
               CM-SEC-RETURN-CODE      = +0000                           00880000
               CM-SEC-RETURN-MSG-SHORT = 'SEC +0000 ACCESS OK '          00890000
               CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +0000:  '          00900000
               ... && 'RESOURCE EXISTS- USER CAN ACCESS'                 00910003
            WHEN CVDA-AREA = DFHVALUE(NOTREADABLE)                       00920000
               CM-SEC-RETURN-CODE      = +3502                           00930000
               CM-SEC-RETURN-MSG-SHORT = 'SEC +3502 NOTREADABLE'         00940000
               CM-SEC-RETURN-MSG-LONG  = 'EESM:  USER NOT AUTH'          00950015
               ... && 'ORIZED FOR UPDATE OR DELETION.      '             00960015
                                                                         00970000
PARA     2100-INVREQ-CONDITION                                           00980000
/*       /*HANDLES CONDITION FOR INVREQ/*                                00990000
         CM-SEC-RETURN-CODE      = +3601                                 01000000
         CM-SEC-RETURN-MSG-SHORT = 'SEC +3601 INVREQ  '                  01010000
         CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3601:  '                01020000
         ... && 'INVREQ - SEVERE ERROR '                                 01030003
         ESCAPE                                                          01040000
                                                                         01050000
PARA     2200-LENGERR-CONDITION                                          01060000
/*       /*HANDLES CONDITION FOR LENGERR/*                               01061000
         CM-SEC-RETURN-CODE      = +3602                                 01070000
         CM-SEC-RETURN-MSG-SHORT = 'SEC +3602 LENGERR '                  01080000
         CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3602:  '                01090000
         ... && 'LENGTH ERROR - REVIEW LINKAGE '                         01100003
         ESCAPE                                                          01110000
                                                                         01120000
PARA     2300-NOTFND-CONDITION                                           01130000
/*       /*HANDLES CONDITION FOR NOTFND /*                               01131000
         CM-SEC-RETURN-CODE      = +3503                                 01140000
         CM-SEC-RETURN-MSG-SHORT = 'SEC +3503 RSRC NOTFND '              01150000
         CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3503:  '                01160000
         ... && 'NO ACCESS - RESOURCE NOT FOUND '                        01170003
         ESCAPE                                                          01180000
                                                                         01190000
PARA     2400-QIDERR-CONDITION                                           01200000
/*       /*HANDLES CONDITION FOR QIDERR /*                               01201000
         CM-SEC-RETURN-CODE      = +3603                                 01210000
         CM-SEC-RETURN-MSG-SHORT = 'SEC +3603 QIDERR '                   01220000
         CM-SEC-RETURN-MSG-LONG  = 'ITSSD916 RC +3603:  '                01230000
         ... && 'QUEUE ID ERROR - SEVERE '                               01240003
         ESCAPE                                                          01250000
                                                                         01260000
```

3.1.2.2 Cobol Coding Example

```
       IDENTIFICATION DIVISION.
       PROGRAM-ID.    IBOX1111.
       AUTHOR.        IBOX PROJECT TEAM.
```

```
       INSTALLATION.  BC/BS OF SC.
       DATE-WRITTEN.  FEBRUARY, 2004.
       DATE-COMPILED.
      ***************************************************************
      *             INTER-PLAN TELEPROCESSING SERVICES  (ITS)       *
      *                                                             *
      *   MODULE:       IBOX1111                                    *
      *   NAME:         IBOX CICS SECURITY MODULE                   *
      *                                                             *
      *   APPLICATION:  IBOX                                        *
      *   TYPE:         CICS                                        *
      *   FUNCTION:     LINK TO THIS MODULE TO INTERROGATE A USER'S  *
      *                 SECURITY AUTHORIZATION; FIRST USE IS FOR    *
      *                 COLLECTION ID AUTHORIZATION CHECKING; MAY   *
      *                 BE USED FOR OTHER SECURITY CHECKS IN FUTURE; *
      *                                                             *
      *   MODIFICATION                                              *
      *                                                             *
      *    DATE: 02/29/04 01.0 INITIAL RELEASE                      *
      *                                                             *
      *   NOTES:        REFER TO DFHCOMMAREA FOR DESCRIPTION OF     *
      *                 LINKAGE FIELDS AND POSSIBLE RETURN CODES    *
      *                                                             *
      ***************************************************************

       ENVIRONMENT DIVISION.

       DATA DIVISION.

       WORKING-STORAGE SECTION.

       01  FILLER                              PIC X(50)
           VALUE '*** IBOX1111 WORKING STORAGE BEGINS HERE=========>'.

       01  FILLER                              PIC X(50)
           VALUE '*** IBOX1111 SECURITY DEFINITIONS START==========>'.

       01  RESCLAS-VALUE                PIC X(08)       VALUE SPACES.
       01  CVDA-AREA                    PIC S9(8)  COMP VALUE 0.
       01  CVDA-LOG                     PIC S9(8)  COMP VALUE 0.
       01  CVDA-NOLOG                   PIC S9(8)  COMP VALUE 0.
       01  RESOURCE-VALUE               PIC  X(8)       VALUE SPACES.
       01  RESOURCE-LENGTH              PIC S9(8)  COMP VALUE 0.

       01  FILLER                              PIC X(50)
           VALUE '<===IBOX1111 SECURITY DEFINITIONS END************'.
       01  FILLER                              PIC X(50)
           VALUE '<===IBOX1111 WORKING STORAGE END*****************'.
```

```
*****************************************************************
***                  LINKAGE DOCUMENTATION
***
***  CM-SEC-WRITE-VIOL-TO-LOG-SW
***                 SET TO 'Y' TO WRITE TO LOG IF SECURITY ERROR
***                 SET TO 'N' IF YOU DO NOT WANT TO WRITE TO LOG
***                   *** USE 'N' FOR TESTING IF POSSIBLE ***
***
***  CM-SEC-RESOURCE-CLAS-VALUE
***                 '$CICSFLD' IS USED FOR COLLECTION ID RACF CHK
***                 '????????' OTHER VALUES MAY BE USED IN FUTURE
***                 '????????' OTHER VALUES MAY BE USED IN FUTURE
***
***  CM-SEC-RESOURCE-VALUE
***                 'ITSSP001' IS AN EXAMPLE OF COLLECTION ID
***                            USED WITH $CICSFLD FOR COLLID
***                            RACF SECURITY CHECK
***                 '????????' OTHER RESOURCE VALUES MAY BE
***                            USED IN FUTURE (MAY NEED CODE CHG)
***
***  CM-SEC-RESOURCE-LENGTH
***                 +0008      IS USED FOR COLLID RACF CHECK
***                 +????      OTHERS USED IN FUTURE (MAY
***                              REQUIRE CODE CHANGE)
***
***  CM-SEC-EXIT-NAME           SET TO SPACES FOR NOW
***
***  CM-SEC-RETURN-CODE
***  CM-SEC-RETURN-CVDA-AREA
***  CM-SEC-RETURN-MSG-SHORT
***  CM-SEC-RETURN-MSG-LONG
***
***    RETURN CODE EXPLANATIONS
***
***      ** NOTE: SOME OF THESE PERTAIN TO THE COLLID RACF
***      ** CHECK; MAY BE USED DIFFERENTLY FOR OTHER RESOURCE
***      ** CLASSES USED IN FUTURE
***
***    +0000  GOOD CALL   (FOR COLL ID CHK, THE COLLID DOES EXIST
***                          AND THE USER IS AUTHORIZED FOR IT)
***
***             THE 3500 SERIES IS RESERVED FOR WARNING MESSAGES
***    +3502  NOTREADABLE (FOR COLLID CHK, THE COLLID EXISTS BUT
***                          THE USER IS NOT AUTHORIZED FOR IT)
***    +3503  NOTFND      (FOR COLLID CHK, USER WAS NOT AUTHORIZED
***                          FOR THAT COLLECTION ID, AND THE
***                          COLLID PROBABLY DOESN'T EXIST YET)
```

```
***    +3599  UNKNOWN     (NOT ABLE TO DETERMINE USERS AUTHORITY
***                          FOR THAT COLLECTION ID)
***
***             THE 3600 SERIES IS RESERVED FOR SEVERE MESSAGES
***
***    +3601  INVREQ   CICS HANDLE CONDITION
***    +3602  LENGERR  CICS HANDLE CONDITION - PROBABLY A BAD
***                      RESOURCE LENGTH IN THE LINKAGE AREA
***    +3603  QIDERR   CICS HANDLE CONDITION
***    +3604  BADLOGSW (CALLING PROGRAM MUST SET LOG SWITCH TO
***                           'Y' OR 'N')
***                                          ***************
***                                          *LENGTH = +106*
***                                          ***************
 LINKAGE SECTION.

 01  DFHCOMMAREA.

     05  CM-SEC-WRITE-VIOL-TO-LOG-SW              PIC  X(1).
     05  CM-SEC-RESOURCE-CLAS-VALUE               PIC  X(8).
     05  CM-SEC-RESOURCE-VALUE                    PIC  X(8).
     05  CM-SEC-RESOURCE-LENGTH                COMP PIC S9(8).
     05  CM-SEC-EXIT-NAME                         PIC  X(8).

     05  CM-SEC-RETURN-CODE                    COMP PIC S9(4).
     05  CM-SEC-RETURN-CVDA-AREA               COMP PIC S9(8).
     05  CM-SEC-RETURN-MSG-SHORT                  PIC X(21).
     05  CM-SEC-RETURN-MSG-LONG                   PIC X(50).

 PROCEDURE DIVISION.

*****************************************************************
*    PROCEDURE DIVISION HERE                                    *
*****************************************************************

     PERFORM 1000-INITIALIZATION
        THRU 1000-EXIT

     IF CM-SEC-RETURN-CODE = +3699
         PERFORM 2000-MAINLINE
            THRU 2000-EXIT
     END-IF

     PERFORM 3000-FINALIZATION
        THRU 3000-EXIT

     GOBACK.
```

```
 1000-INITIALIZATION.

*****************************************************************
*    VALIDATE INPUT LINKAGE FIELDS AS REQUIRED;                 *
*    WE WILL ASSUME RC = 3699 UNLESS FOUND OTHERWISE            *
*****************************************************************

     MOVE +3699                     TO  CM-SEC-RETURN-CODE
     MOVE 'SEC +3699 BAD INITIAL'   TO  CM-SEC-RETURN-MSG-SHORT
     MOVE 'IBOX1111 RC +3699: ERROR DURING INTIALIZATION     '
                                    TO  CM-SEC-RETURN-MSG-LONG

     MOVE DFHVALUE(LOG)                 TO  CVDA-LOG
     MOVE DFHVALUE(NOLOG)               TO  CVDA-NOLOG

     MOVE CM-SEC-RESOURCE-CLAS-VALUE    TO  RESCLAS-VALUE
     MOVE CM-SEC-RESOURCE-VALUE         TO  RESOURCE-VALUE
     MOVE CM-SEC-RESOURCE-LENGTH        TO  RESOURCE-LENGTH

     IF CM-SEC-WRITE-VIOL-TO-LOG-SW = 'Y'
     OR CM-SEC-WRITE-VIOL-TO-LOG-SW = 'N'
         CONTINUE
     ELSE
         MOVE +3604                     TO  CM-SEC-RETURN-CODE
         MOVE 'SEC +3604 INV LOG SW '   TO  CM-SEC-RETURN-MSG-SHORT
         MOVE 'IBOX1111 RC +3604: LINKAGE LOG SWITCH NOT Y OR N  '
                                        TO  CM-SEC-RETURN-MSG-LONG
     END-IF

 1000-EXIT.
    EXIT.

 2000-MAINLINE.

*****************************************************************
*    MAINLINE FOR PROGRAM PROCESSING                            *
*      - NOW WE WILL ASSUME CODE +3599 (UNKNOWN) FOR NOW        *
*      - SET THE HANDLE CONDITION TRAPS                         *
*      - CALL EITHER THE LOG OR NOLOG VERSION OF SEC QUERY      *
*          DEPENDING ON WHAT CALLING PROGRAM REQUESTED          *
*****************************************************************

     MOVE +3599                     TO  CM-SEC-RETURN-CODE
     MOVE 'SEC +3599 ACCESS UNKN'   TO  CM-SEC-RETURN-MSG-SHORT
     MOVE 'IBOX1111 +3599: NO USER ACCESS - REASON UNKNOWN   '
                                    TO  CM-SEC-RETURN-MSG-LONG
     EXEC CICS HANDLE CONDITION
```

```
            INVREQ(2100-INVREQ-CONDITION)
            LENGERR(2200-LENGERR-CONDITION)
            NOTFND(2300-NOTFND-CONDITION)
            QIDERR(2400-QIDERR-CONDITION)

        END-EXEC

        IF CM-SEC-WRITE-VIOL-TO-LOG-SW = 'Y'

            EXEC CICS QUERY SECURITY
                 RESCLASS(RESCLAS-VALUE)
                 RESID(RESOURCE-VALUE)
                 RESIDLENGTH(RESOURCE-LENGTH)
                 READ(CVDA-AREA)
                 LOGMESSAGE(CVDA-LOG)
            END-EXEC

        ELSE

            EXEC CICS QUERY SECURITY
                 RESCLASS(RESCLAS-VALUE)
                 RESID(RESOURCE-VALUE)
                 RESIDLENGTH(RESOURCE-LENGTH)
                 READ(CVDA-AREA)
                 LOGMESSAGE(CVDA-NOLOG)
            END-EXEC

        END-IF

        MOVE CVDA-AREA                    TO  CM-SEC-RETURN-CVDA-AREA

        EVALUATE TRUE

          WHEN CVDA-AREA = DFHVALUE(READABLE)

            MOVE +0000                    TO  CM-SEC-RETURN-CODE
            MOVE 'SEC +0000 ACCESS OK  '  TO  CM-SEC-RETURN-MSG-SHORT
            MOVE 'IBOX1111 RC +0000: RESOURCE EXISTS-USER CAN ACCESS'
                                          TO  CM-SEC-RETURN-MSG-LONG

          WHEN CVDA-AREA = DFHVALUE(NOTREADABLE)

            MOVE +3502                    TO  CM-SEC-RETURN-CODE
            MOVE 'SEC +3502 NOTREADABLE'  TO  CM-SEC-RETURN-MSG-SHORT
            MOVE 'IBOX1111 +3502: RESOURCE EXISTS-USER NOT AUTHORZD '
                                          TO  CM-SEC-RETURN-MSG-LONG

        END-EVALUATE
```

```
 2000-EXIT.
     EXIT.

 2100-INVREQ-CONDITION.

*****************************************************************
*    HANDLES CONDITION FOR INVREQ                               *
*****************************************************************

     MOVE +3601                     TO  CM-SEC-RETURN-CODE
     MOVE 'SEC +3601 INVREQ     '   TO  CM-SEC-RETURN-MSG-SHORT
     MOVE 'IBOX1111 RC +3601: INVREQ - SEVERE ERROR          '
                                    TO  CM-SEC-RETURN-MSG-LONG
     PERFORM 3000-FINALIZATION
        THRU 3000-EXIT.

 2100-EXIT.
     EXIT.

 2200-LENGERR-CONDITION.

*****************************************************************
*    HANDLES CONDITION FOR LENGERR                              *
*****************************************************************

     MOVE +3602                     TO  CM-SEC-RETURN-CODE
     MOVE 'SEC +3602 LENGERR    '   TO  CM-SEC-RETURN-MSG-SHORT
     MOVE 'IBOX1111 RC +3602: LENGTH ERROR - REVIEW LINKAGE  '
                                    TO  CM-SEC-RETURN-MSG-LONG
     PERFORM 3000-FINALIZATION
        THRU 3000-EXIT.

 2200-EXIT.
     EXIT.

 2300-NOTFND-CONDITION.

*****************************************************************
*    HANDLES CONDITION FOR NOTFND                               *
*****************************************************************

     MOVE +3503                     TO  CM-SEC-RETURN-CODE
     MOVE 'SEC +3503 RSRC NOTFND'   TO  CM-SEC-RETURN-MSG-SHORT
     MOVE 'IBOX1111 RC +3503: NO ACCESS - RESOURCE NOT FOUND '
                                    TO  CM-SEC-RETURN-MSG-LONG
     PERFORM 3000-FINALIZATION
        THRU 3000-EXIT.
```

```
 2300-EXIT.
     EXIT.

 2400-QIDERR-CONDITION.

*****************************************************************
*    HANDLES CONDITION FOR QIDERR                               *
*****************************************************************

     MOVE +3603                     TO  CM-SEC-RETURN-CODE
     MOVE 'SEC +3603 QIDERR     '   TO  CM-SEC-RETURN-MSG-SHORT
     MOVE 'IBOX1111 +3603: QUEUE ID ERROR - SEVERE           '
                                    TO  CM-SEC-RETURN-MSG-LONG
     PERFORM 3000-FINALIZATION
        THRU 3000-EXIT.

 2400-EXIT.
     EXIT.

 3000-FINALIZATION.

*****************************************************************
*    FINALIZATION;                                              *
*    RETURN TO CICS                                             *
*****************************************************************

     EXEC CICS RETURN
     END-EXEC.

 3000-EXIT.
     EXIT.
```

3.1.3 Application Level Security Tables

The following tables can be interfaced by systems that utilize non-RACF security applications for security below the transaction level. The tables help ensure that those systems are in sync with RACF, concerning transfers and terminations, when requiring the modification or deletion of user security access within the applications. Details on how these files are maintained can be obtained from the RACF Administrator.

RACF User IDs are deleted for one of the following reasons:

1. Termination
2. External customer no longer requires access
3. 90 days of inactivity
4. Received requests

Terminations

This file contains an audit trail of RACF-defined User ID deletion activity.

```
BC.ISEC.RACF.DELFILE.GxxxxVxx (z/OS Corporate system)
CDS.ISEC.RACF.DELFILE.GxxxxVxx (z/OS Medicare system)

Col.   Len.  Data
1      8     User ID
10     3     OPID
15     20    Employee Name
40     4     Employee Number (XXXX) for externals
45     10    Delete date (yyyy-mm-dd)
60     8     Delete time (hh:mm:ss)
68     4     Cost Center
72     8     Company based group
80     8     Role based group
```

Active Users

This file contains a complete list of active RACF-defined User IDs.

```
BC.ISEC.ACTIVE.RACF.USERIDS (z/OS Corporate system)
CDS.ISEC.ACTIVE.RACF.USERIDS (z/OS Medicare system)

Col.   Len.  Format      Contents              Comment
1      8     Character   User ID
10     8     Character   Default RACF Group
20     4     Character   Employee Number       Blank if unable to determine
25     3     Character   OPID                  Blank if unable to determine
30     4     Character   Cost Center           Blank if unable to determine
35     10    Character   User's first name
45     10    Character   User's last name
55     20    Character   Name from RACF database
76     3     Character   RACF Protected flag   If “PRO” ID is RACF Protected
80     1     Character   Revocation Flag       If “Y” User ID is revoked
```

Transfers

This file contains an audit trail regarding all transfers that have occurred.

```
BC.ISEC.HRCOMPAR.LISTING.GxxxxVxx (z/OS Corporate system)
CDS.ISEC.HRCOMPAR.LISTING.GxxxxVxx (z/OS Medicare system)
Example:
SRC    EMP#   CO     DV     CC     JCODE        USER NAME    MANAGER      MGR EMP
```

```
OLD    0000   033   39   565   IF127        Jane Doe     John Doe     A123
NEW    0000   001   30   304   MB134        Jane Doe     Jill Doe     B123
```