BCU-S03-ACCESS CONTROL STANDARD

Table of Contents

1.0 PURPOSE

The purpose of this standard is to outline access control within BCU. BCU implements access control across its networks, IT systems and services in order to provide authorized, granular, auditable, and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity, and availability in accordance with *BCU-S01-Security Standard*. Access control systems are in place to protect the interests of all authorized users of BCU IT systems by providing a safe, secure, and accessible environment in which to work.

1.1 SCOPE

The scope of this standard applies to all users of information resources, electronic and computing devices, and network resources to conduct BCU business or interact with internal networks business systems, whether such system is owned or lease by BCU, the employee, or a third party. This standard applies to employees, contractors, consultants, temporary employees, and other workers at BCU, including all personnel that are affiliated with third parties. This standard applies to all equipment that is owned or leased by BCU.

2.0 GENERAL ACCESS CONTROL

Access control standards for BCU information systems are established in a manner that balances restrictions to prevent unauthorized access to information and services against the need for unhindered access for authorized users. BCU shall provide all employees, contractors, consultants, temporary employees, and interns with on-site access to the information they need to carry out their responsibilities in an effective and efficient manner as possible.

2.1 GENERIC ACCOUNTS

Generic accounts, or group and/or shared accounts, shall not normally be permitted as any means of access to BCU data, but may be granted under exceptional circumstances if sufficient other controls of access are in place. The use of generic and/or shared accounts shall not be used in any way to manage BCU resources and/or infrastructure. The BCU Security Team, in addition to Management, is required to approve this exception.

2.2 PRIVELEGED ACCOUNTS

The allocation of privileged rights (e.g., local administrator, domain administrator, Global Administrator, super user, root, sa, etc.) shall be restricted, controlled, not provided by default, used on an as-needed basis, and audited. Authorization for the use of privileged rights and accounts shall only be provided explicitly, upon written request from the department or group manager, and will be documented by the system owner. The Identity and Access Management (IAM) team shall manage all privileged access. Access to privileged accounts shall be audited quarterly.

Privileged access shall only be permitted on a dedicated System Administrator (SA) account. SA accounts are created for all new Infrastructure and Operations department and Security department personnel. All others require approval by the Senior Manager, Security – Physical and IAM. SA accounts shall be deactivated upon termination.

SA account credentials shall be housed within a dedicated privileged access management (PAM) system and checked-out when needed. Passwords for SA accounts shall be rotated upon check-in.

SA account sessions are monitored and recorded by the PAM system, and sessions shall be reviewed by the IAM team regularly.

2.3 LEAST PRIVILEGE AND NEED TO KNOW

All access rights will be provided following the principles of least privilege and need to know. This ensures that the user can access only the information and resources that are necessary for their legitimate purpose and job function.

2.4 USER ACCOUNTS

All access to BCU resources and services will be provided through the provision of a unique user account and complex password. Passwords must meet the minimum complexity requirements as defined in *BCU-S05-Password Standard*. Users may have multiple user accounts, and as such shall be provided a unique user account for each resource, as necessary. Additionally, passwords across multiple accounts should never be reused, both internally and externally to BCU information resources.

2.5 THIRD PARTIES

All third parties that are provided with accounts to access BCU Security resources shall be granted upon manager approval. Third parties shall solely be provided access to the systems and/or data that they have been contracted to handle, in accordance with least privilege and need to know principles. Third party accounts will be removed at the end of the contract or when they are no longer required. Third party access shall follow standards outlined in *BCU-S13-General Controls for Vendor Management Guideline*.

2.6 ACCESS TO SENSITIVE DATA

Access to sensitive data, as classified in *Section 4* of the *BCU-S01-Security Policy*, is limited to authorized users whose job responsibilities require it, as determined by law, contractual agreement, or *BCU-S01-Security Policy*. The responsibility to implement access restrictions lies with the information and data owner.

Role-based access control, or RBAC, shall be used as the method to secure access to all file-based resources contained within BCU's domain and administered by BCU. Additionally, RBAC and the principle of least privileged shall be used as a method to secure access to all database (e.g., SQL) resources contained within BCU's environment and that are administered by BCU. Access rights to such groups (e.g., SQL Administrator, SQL Datawarehouse Admin, etc.) shall be audited at least quarterly.

2.7 GUIDELINES FOR USE OF ACCOUNTS

All users accessing BCU resources are expected to be familiar with and abide by BCU policies, procedures, standards, and guidelines for appropriate and acceptable use of BCU networks and systems. Concurrent logins (e.g., same user ID, same password) are not permitted and limited to only specific situations. Additionally, sharing of user accounts and passwords is prohibited. The use of privileged accounts as primary method of authentication is prohibited. Privileged accounts should never be provided to third parties, contractors, vendors, etc. Any exception to this standard must be approved by the BCU Security Team.

2.8 REMOTE ACCESS

Access for remote users and BCU's Citrix environment shall be subject to authorization by the users reporting manager and will be provided in accordance with *BCU-S14-Remote Access Standard, BCU-S13-General Controls for Vendor Management Guideline,* and *BCU-S01-Security Policy*. No uncontrolled external access shall be permitted to any network device or networked system.

2.9 UNAUTHORIZED ACCESS

Unauthorized access of BCU or Baxter data files, networks, and applications, or attempting to access credit union data without specific authorization, is prohibited. This includes access of third-party computers or databases, using credit union computers. Any form of tampering, including snooping and hacking, to gain access to computers is a violation of BCU standards. Employees are required to either password protect or turn their computer off at the end of the day, and when

left unattended. In addition, computer users must take other reasonable precautions to prevent unauthorized access of credit union computers and information.

3.0 ACCESS MANAGEMENT

3.1 ACCESS DEFINITIONS

Access provisioning and deprovisioning is managed by a combination of automated and manual processes. Access to BCU resources and data is determined by a combination of department and role. Establishing, approving, and updating appropriate access privileges at the department level within key applications is the responsibility of dedicated application governance committees. These privileges are documented on the user access matrix maintained by the IAM team.

3.2 ONBOARDING

Onboarding new users is initiated via either Service Desk form or the Human Resources Information System (HRIS), and BCU Human Resources approval is required for new employees and contractors. Creation of the new user's directory account is automated via the IAM system, along with appropriate access to additional systems integrated with the IAM system. IAM team personnel perform manual provisioning of accounts in other systems per the user access matrix.

3.3 CHANGES

Role changes requiring access changes follow the same process as onboarding. Access changes for systems managed via the IAM system shall occur on the effective date of the change. Access changes for systems managed manually shall occur a maximum of 48 hours prior to the effective date.

3.4 TERMINATIONS

Terminations can be initiated via Service Desk form, the HRIS, or by BCU Human Resources verbally or in writing. Directory accounts are deactivated at the requested date and time for planned terminations, or immediately if required. Upon notification of termination, all manual account deactivations shall be completed within 24 hours of termination.

4.0 ACCESS REVIEWS

4.1 CERTIFICATION CAMPAIGNS

Certification campaigns are conducted quarterly via the IAM tool, starting on the first business day of each quarter. All personnel with direct reports shall conduct their reviews within 30 days of the initiation of the campaign. Any incomplete reviews are automatically approved by the IAM tool upon closure of the campaign. A report of personnel who have failed to complete their campaign shall be sent to the CSO. Failure to complete an assigned certification campaign can result in disciplinary action.

The IAM team shall verify and, if necessary, update the user access matrix prior to the initiation of quarterly campaigns. The matrix shall be made available to all personnel conducting certification campaigns. The IAM team shall also send a reminder to complete the campaign 7 days prior to the campaign closing date.

5.0 STANDARD COMPLIANCE

The BCU Security Team will verify compliance to this standard through various methods, including but not limited to, periodic walk-through's, penetration testing, business reporting tools, internal and external audits, and feedback to the

standard owner. Any exception to this standard must be approved the BCU Security Team in advance. An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

6.0 DOCUMENT ADMINISTRATION

6.1 DOCUMENT OWNER

This document is owned by the Security Team, which is responsible for its content and maintenance.

6.2 DOCUMENT REVIEW

This document is subject to review on an annual (or more frequent) basis to validate that its content remains relevant and up to date. Significant or material changes to this document must be reviewed and approved by the Member Data Security Committee as described in *BCU-S01-Security Policy*, Section 3, *Roles, and Responsibilities.*

6.3 CHANGE HISTORY

Version	Change	Author	Date
1.0	Initial version	Martin Hetzel	12/9/2016
1.0	Reviewed	Martin Hetzel	4/12/2017
1.0	Reviewed, added Vendor reference to BCU-IS25-Vendor Access	Martin Hetzel	5/9/2018
1.0	Reviewed; minor grammar updates	Martin Hetzel	7/9/2019
2.0	Annual review	Marco Colon	8/8/2021
3.0	Reviewed, changed audit frequency from monthly to quarterly, other grammar and wording updates	Steve Jauregui	7/13//2022
4.0	Added statement on IAM team managing privileged accounts	Steve Jauregui	9/29/2023
5.0	Added access provisioning, privileged access management, and access review details	Steve Jauregui	6/28/2024

6.4 APPROVAL HISTORY

Version	Name	Title	Date
1.0	Pete Sedgwick	Dir Cloud and Information Security	12/9/2016
1.0	Joe Suareo	CISO	5/25/2018
1.0	Jeff Johnson	CIO	7/10/2019
2.0	Stephenie Southard	CISO	2/2/2020
3.0	Stephenie Southard	CISO	7/13/2021
4.0	Stephenie Southard	CISO	7/16/2022
5.0	Stephenie Southard	CSO	07/08/2024