BCU-S14-REMOTE ACCESS STANDARD

Table of Contents

1.0 PURPOSE

The purpose of this standard is to define standards for connecting to BCU's security network from remote locations. These standards are designed to minimize the potential exposure to BCU from damages which may result from unauthorized use of BCU resources. Damages include, but are not limited to, the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical BCU systems, the loss of member data, etc.

1.1 OVERVIEW

BCU is committed to managing and maintaining the confidentiality, availability, and integrity of information technology networks, systems, and applications. This includes establishing guidelines for remote access to BCU's critical information assets maintained with the IS department. Remote access is the process of accessing information resources from networks that are not controlled by BCU. This standard defines the appropriate security measures that are required for an authorized user to remotely connect to the BCU secure network.

1.2 SCOPE

This standard applies to all BCU employees, contractors, vendors, and agents with a BCU-owned or personally owned computer or workstation used to connect to the BCU network. This standard applies to remote access connections used to do work on behalf of BCU, including reading or sending email and viewing internal resources. Smartphones and tablets (both company owned and BYOD) are included in scope. Users are required to enroll with Intune and agree to security standards before being able to synchronize with company data. These devices can also log into ROAM through the Citrix mobile app.

2.0 STANDARD

It is the responsibility of BCU employees, contractors, vendors, and agents with remote access privileges to BCU's secure network to ensure that their remote access connection is given the same consideration as the user's on-site connection to BCU.

2.1 GENERAL

Remote access to BCU's secure network is controlled through the use of Citrix Published Desktops and Citrix Published Apps. Access to BCU's secure network is done via https://bcuroam.cloud.com/.

All users (BCU employees, contractors, vendors, and agents) are required to follow and comply with the following standards that provide details of protecting information when accessing BCU's secure network via remote access methods, and provide acceptable use of the BCU secure network:

- Acceptable Use Standard
- Access Control Standard
- Handling Sensitive Data Standard
- Encryption Standard
- Authentication & Password Standard
- (Vendors) Vendor Access Standards
- Mobile Device Standard
- Security Policy

2.2 REQUIREMENTS

- Personal use of BCU owned equipment is discouraged and prohibited. Such as letting others use BCU laptops for schoolwork or online learning, shopping, etc.

- All secure remote access must be strictly controlled using encrypted connections, strong passphrases, and multifactor authentication (also referred to as two-factor authentication). Users must be in compliance with *BCU-S05-Password Standard* for required authentication standards
- All authorized users shall protect their login and password and shall not share with anyone.
- While using a BCU-owned computer to remotely connect to BCU's secure network, all authorized users shall ensure that the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized User or Third Party.
- Any reconfiguration of a home user's equipment for the purpose of split-tunneling (or similar) is not permitted at any time.
- When using a wireless network on personal networks to connect to BCU secure network, the wireless connection must be encrypted using, at minimum, WPA2 and must be password protected.
- The mapping of network drives and file transfers outside of BCU's secure network is strictly prohibited.
- Any use of external resources to conduct BCU business must be approved in advance by the BCU security Department and the appropriate business unit manager.
- All devices that connect to BCU's secure network via remote access technologies must use and maintain the most up-to-date anti-virus software, including any personal devices.
- All devices that connect to BCU's secure network via remote access technologies must use and maintain the most up-to-date operating system and security updates, including any personal devices.
- Users are required to work with the Service Desk or others in IT to bring their device to compliance in a timely fashion.
- Any personal equipment that is used to connect to BCU's secure network must meet the requirements of BCU-owned equipment for remote access, as stated in section 2.3, Employee-Owned Computers.
- All third-party connections must comply with the requirements as stated in the Vendor Access Standards and Third-Party Data Security Standards.
- **Any authorized users with remote access privileges to BCU's secure network must not use non-BCU email accounts (e.g., Gmail, Hotmail, Yahoo), or other external resources to conduct BCU business, thereby ensuring that official business is never confused with personal business.**
- In public environments, all users should take precautions to prevent unwanted viewing of device's screen by unauthorized users.
- Employees should not use public WIFI's while conducting work "business." Employees should use mi-fi or private network devices to connect.
- Sensitive, Confidential, or Secret BCU data must not be read, discussed, or otherwise exposed in public places, including, but not limited to; restaurants, public transportation, or other public places where unauthorized people might discover it.
- Public computers or devices, such as library PC's or kiosks, are restricted from use to access BCU systems.
- Any authorized users shall not transfer confidential, sensitive, or secrete data from BCU's secure network to an unsecured device or location.
- Any users or organization who wish to implement non-standard Remote Access solutions to BCU's secure network must obtain prior approval from the BCU security Department.

2.3 EMPLOYEE-OWNED COMPUTERS

Any employee-owned computer that is located within an employee's residence and used for BCU related activities are subject to compliance within this standard. All devices not owned by BCU and used to connect to the BCU secure network or are used to conduct BCU business must be used in compliance with all BCU standards, policies, and procedures. BCU retains the right to inspect any data sent into BCU's network or that is extracted from BCU's network. The following minimum requirements must be met.

- Appropriate anti-virus and anti-malware solution is installed
- Appropriate supported operating system is current and kept up to date.

- Ensure a firewall is installed and enabled
- Ensure that third-party applications are kept up to date
- Unsupported operating systems will not be allowed to access BCU's remote environment
- Screen saver policies and/or other safeguards must be followed if a machine must be left unattended while connected or logged into the BCU network.
- Mobile devices must meet the requirements as denoted in *BCU-S06-Mobile Device Standard*.

3.0 STANDARD COMPLIANCE

The BCU Security Department 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 by the BCU Security Department in advance. An employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

4.0 DOCUMENT ADMINISTRATION

4.1 DOCUMENT OWNER

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

4.2 DOCUMENT REVIEW

This document is subject to be reviewed 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*.

4.3 CHANGE HISTORY

Version	Change	Author	Date
1.0	Initial version	Martin Hetzel	
2.0	Updates	Stephenie Southard	6/10/21
2.0	Annual review	Mike Lim	8/18/21
2.0	Annual Review	Mike Lim	10/7/2022
3.0	Minor typos, updated ROAM URL	Steve Jauregui	9/29/2023
3.0	Reviewed	Steve Jauregui	6/28/2024

4.4 APPROVAL HISTORY

Version	Name	Title	Date
1.0	Joe Suareo	CISO	11/2/2018
1.0	Jeff Johnson	CIO	07/19/19
2.0	Stephenie Southard	CISO	08/18/21
2.0	Stephenie Southard	CISO	10/7/2022
3.0	Stephenie Southard	CSO	10/9/2023
3.0	Stephenie Southard	CSO	07/08/2024