Butte Glenn Community College Information Technology Standard Operating Procedures

Subject: Remote Access & Virtual Private Network Connectivity

Section: Information Technologies *Effective Date: 11/5/24*

Sub-Section: Security *Review Date: 11/6/24*

Version History

Version #	History of Changes	Author	Date
1.0	Initial Policy	W. Brandt	10/15/24

Purpose

This procedure provides guidelines for Remote Access and/or Virtual Private Network (VPN) connections to the Butte-Glenn Community College District (BGCCD) Information Systems network. These guidelines are designed to minimize the potential exposure to BGCCD from damage which may result from unauthorized use of BGCCD resources.

Policy Statement

Anyone given the privilege of using BGCCD computing, and information systems resources is expected to act in a responsible manner by complying with all BGCCD policies and procedures, relevant laws, and contractual agreements related to computers, networks, software, and computer information. This procedure applies to anyone who uses, or wishes to use, the BGCCD Remote Access & Virtual Private Network services.

Procedure

Specifically authorized stakeholders and specifically authorized third parties may utilize the benefits of Remote Access and VPN's which are a "user managed service". This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, updates, and/or patches, and paying associated fees. Further, every authorized VPN user must read, acknowledge, and abide by BGCCD Administrative Procedure AP-3720 Computer and Network Use Procedure.

Remote/VPN Access: Remote access is granted for authorized BGCCD work only as determined by the department Dean or Director, BGCCD Security Manager, and after review and approval by the Chief Technology Officer of Information Systems or designee(s). All authorized BGCCD stakeholders and authorized third parties shall comply with this procedure which details the safeguards that must be employed:

- **Secured Access:** Any remote/VPN access to the BGCCD WAN/LAN is accomplished via a secure remote access method provided by BGCCD and managed and maintained by BGCCD Information Technology Systems.

- **Unauthorized Access**: Authorized users shall be responsible for ensuring that unauthorized person(s) do not access the BGCCD WAN/LAN. Should an unauthorized event occur, the user shall report it immediately, and in any case no later than within 24 hours of discovery. Reports and notifications shall be made to the BGCCD Chief Technology Officer, Security Manger, or their designee(s).

- **Split Tunneling:** Dual or split tunneling is not permitted during a remote/VPN connection to the BGCCD WAN/LAN. Only one network connection shall be permitted.

- **Virus Protection:** Anyone with remote/VPN access to the BGCCD WAN/LAN from a BGCCD or privately owned computer(s) will exercise due diligence in ensuring that the systems, both hardware and software, are free from viral infection. Where possible, BGCCD may employ technical measures to ensure compliance.

- **Software and Hardware Updates/Patches:** Anyone with remote/VPN access to the BGCCD WAN/LAN from a BGCCD or privately owned computer(s) will exercise due diligence in ensuring that the systems, both hardware and software, are fully updated with vendor required and recommended patches and updates. Where possible, BGCCD may employ technical measures to ensure compliance.

- **Access Termination:** When an authorized user no longer needs access, terminates BGCCD employment or transfers to another department, office or agency, and/or in the instance when an authorized user is a third-party vendor whose contract has ended or service is no longer required, all remote access services and systems rights shall be terminated. Users shall notify the BGCCD Chief Technology Officer, Security manager, or their designee(s) immediately upon the occurrence of any event such as project cessation, change of employment, etc. that necessitates access termination. BGCCD owned hardware shall be returned to BGCCD and software shall be permanently deleted from any equipment not owned by BGCCD.

- **Account Requests and User Responsibility:** User accounts will be created only at the request of a department Dean or Director and with the approval of the BGCCD Chief Technology Officer, Security Manager, or their designee(s). Requests shall be submitted in writing using the Remote / VPN Access Request Form found as Appendix A to this procedure. Requests shall be made a minimum of ten (10) business days before access is needed.

Non-BGCCD Personnel Accounts: Accounts for authorized users that are not directly employed by BGCCD (i.e. customers, contractors, consultants, vendors, etc.) must be approved by the requesting department's Dean or Director and the Chief Technology Officer, Security Manager, or their designee(s). Additionally, a copy of the Remote / VPN Access Request Form and any pertinent confidentiality agreement(s) must be signed by the individual and/or the designated approving authority and returned to the BGCCD Chief Technology Officer, Security Manager, or their designee(s). Accounts will not be issued until this process has been completed. Requests shall be made a minimum of ten (10) business days before the account access is needed.

Username and Password Authentication: VPN access is controlled using username and password authentication. The password will be initially assigned by the BGCCD Chief Technology Officer, Security Manager, or their designee(s). Each user must have a unique account. Shared accounts are not permitted. Exceptions may be considered and discussed with the BGCCD Chief Technology Officer, Security Manager, or their designee(s) for approval in limited, defined situations.

Additionally, the user is responsible for maintaining the security and integrity of their unique username and password. Passwords shall be unique and complex according to best practices for password security and shall not be stored or transported in any unsecure non-encrypted method. Authentication methods are subject to change as determined by the BGCCD Chief Technology Officer, Security Manager, or their designee(s).

Multi Factor Authorization: All VPN access requests must utilize multi-factor authentication (MFA) to enhance security measures. Users will be required to use a designated MFA authentication tool approved by BGCCD. The designated tool will be identified by BGCCD Information Technologies department and communicated to all users. Users must ensure that MFA is properly configured and activated on their devices prior to accessing the VPN. Failure to comply with the MFA requirement may result in denial or revocation of VPN access privileges.

Auditing/Monitoring: All users are subject to auditing and monitoring without notice, including review of users' online activity and content accessed. The BGCCD Security Manager shall conduct an annual audit and review of VPN accounts. VPN accounts no longer being used shall be immediately disabled and deleted.

Access Limitations: Remote/VPN access shall be limited to the specific resources requested and approved. Open access via Remote/VPN to BGCCD WAN/LAN resources shall not be permitted.

Connectivity Time Limitations: Remote/VPN users shall be automatically disconnected from the BGCCD network after thirty (30) minutes of inactivity, or any other time period in the BGCCD's discretion. The user shall be required to logon again if reconnection with the network is desired. Artificial network processes that keep the connection open are strictly prohibited. User connections to the VPN shall be limited to an absolute connection time of eight (8) hours per day. Exceptions may be considered and should be reviewed with the BGCCD Chief Technology Officer, Security Manager, or their designee(s)for approval in limited, defined situations. The BGCCD does not guarantee access to the VPN and users may experience delays or downtime; users should have contingency plans in place in the event of interruptions in Remote/VPN access.

Equipment Configuration: As a condition for connection to the BGCCD networks, users seeking access through equipment not owned by BGCCD shall configure the equipment to comply with this procedure and other related BGCCD Information Systems Policies and Procedures. By using VPN technology with personal equipment, users acknowledge that their computer equipment is a de facto extension of the BGCCD network and, as such, when connected shall comply with the same rules and regulations that apply to BGCCD owned equipment (i.e. equipment shall be configured to comply with all BGCCD Information Technology Systems Policies).

Termination of VPN: The applicable BGCCD Department Dean or Director, BGCCD Chief Technology Officer, Security Manager, or their designee(s) may terminate VPN services at any time for any reason. Users do not have an expectation of continued access.

Enforcement:
Violations or activities in contradiction to this procedure will result in loss of all Remote Access and Virtual Private Network Connections. Additionally, further disciplinary action may result, in accordance with the applicable section(s) within the BGCCD Administrative Procedure AP-3720 Computer and Network Use Procedure.

Policy Owner

Security Officer

Standards

1.0 Architecture

Perimeter Architecture

BGCCD shall employ firewalls within the network to protect key BGCCD entry points and data centers.

Remote Access Architecture

In order to control access to the network, remote access gateways must be located at a point that can be controlled and monitored by network operations. This means that remote access gateways must be centralized on a firewall DMZ for control and monitoring.

2.0 Configuration

Failed Login Attempts

Remote access systems shall be configured to allow a maximum of five consecutive failed authentication attempts. After five failed login attempts, the account will be locked for five minutes. After five additional failed login attempts, the account will be locked for fifteen minutes.

Minimum requirements for systems or devices used to access the VPN

- Web browsers shall be the latest version and current with security updates
- Up-to-date anti-virus engine and signature updates
- The system must be virus and malware free
- The system may not be a public use computer such as in a hotel or Internet café
- Current operating system and application security patches

VPN solution requirements

- Encryption must be used in remote access solutions to protect the data from tampering, theft and session hijacking as well as from confidentiality attacks
    - Approved encryption algorithm such as AES
    - Approved protocol such as IPSEC or SSL
- Timeout after 8 hours and re-establishment required even if in use

3.0 Process

Remote Access Approval

- BGCCD staff stakeholders must receive written approval for remote access privileges. To request remote access, the user must complete and submit a VPN access form follow the Access Request process covered in the Access Control Policy.
- Contracting managers are responsible for obtaining remote access approval on behalf of non-employees.

Responsibilities of users of remote access

- Protect all passwords and tokens to prevent unauthorized access of VPN services
- Ensure that no PI, PII, or FERPA information is shared with unauthorized persons
- Review on a regular basis

Policy Approval

Author	Date
W. Brandt	10/15/24

Appendix A

Remote/VPN Account Request/Renewal

Employee/Contractor Name: _____

Department or Vendor Name: _____

Reason for VPN Access: ☐ Colleague ☐ SARS ☐ Reports Server ☐ Other_____

Please complete this form and email it to usersupportservices@butte.edu.

I, the undersigned employee/contractor, is requesting access to Butte-Glenn Community College District's virtual private network (VPN) for the purpose stated above. I understand that access to VPN is granted at the discretion of BGCCD Chief Technology Officer, Security Manager, or their designee(s)and that all network activity may be monitored for security purposes.

I agree to comply with all Butte-Glenn Community College District policies and procedures related to the use of the VPN, including but not limited to this Remote Access & Virtual Private Network Connectivity policy, as well as those related to information security, acceptable use, and confidentiality.

Requestor Print Name: _____
Requestor Signature: _____
Date: _____

Manager, Dean, or Director Approval:
I approve of the above-named individual's request for a VPN account.

Print Name: _____
Signature: _____
Date: _____

Please complete this form and email it to usersupportservices@butte.edu.

This section will be signed after submitting the form to User Support Services.
CTO, Security Manager, Designee Approval:

Print Name: _____
Signature: _____
Date: _____