BULLHOOK
Community Health Center

521 4th Street Havre, Montana 59501 • Phone: 406-395-4305 •Fax: 406-395-5643 • www.bullhook.com

Remote Access Policy 5024

Purpose

The purpose of this policy is to define standards for connecting to Bullhook Community Health Center's (BCHC) network from any host. These standards are designed to minimize the potential exposure to BCHC from damages which may result from unauthorized use of BCHC resources. Damages include the loss of sensitive or company confidential data including Protected Health Information (PHI), intellectual property, damage to public image, damage to critical BCHC internal systems, etc.

Scope

This policy applies to all BCHC workforce members, contractors, vendors and agents with an BCHC-owned or personally-owned computer or workstation used to connect to the BCHC network. This policy applies to remote access connections used to do work on behalf of BCHC, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to DSL, VPN, SSH, SSL.

Policy

Privileges to BCHC's corporate network to ensure that their remote access connection is given the same It is the responsibility of BCHC workforce members, contractors, vendors and agents with remote access consideration as the user's on-site connection to BCHC.

General limited access to the Internet for recreational use by BCHC workforce members is acceptable. The BCHC workforce member shall not perform illegal activities, and shall be responsible for the consequences should the access be misused.

Remote Access Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases

2. At no time should any BCHC workforce member provide their login or email password to anyone.

3. BCHC workforce members and contractors with remote access privileges must ensure that their BCHC-owned or personal computer or workstation, which is remotely connected to BCHC's corporate network, is not connected to any other network at the same time, with the exception of personal wireless networks that are under the complete control of the workforce member.

4. BCHC workforce members and contractors with remote access privileges to BCHC's corporate network must not use non-BCHC email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct BCHC business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a workforce member's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. Non-standard hardware configurations must be approved by the Systems Team, and the Systems Team must approve security configurations for access to hardware.
7. All hosts that are connected to BCHC internal networks via remote access technologies must use the most up-to-date anti-virus software this includes workforce member's own personal computers. Third party connections must comply with Systems Team requirements.
8. Personal equipment that is used to connect to BCHC's networks must meet the same requirements of BCHC-owned equipment for remote access.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the BCHC production network must obtain prior approval from the CEO and the Technology Personnel.

Policy Compliance

Compliance Measurement

The Management Team will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback from BCHC workforce members.

Exceptions

Any exception to the policy must be approved by the CEO, in advance.

Non-Compliance

Any workforce member found to have violated this policy may be subject to disciplinary action.

Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Dual Homing
- Split Tunneling

References:

1. HIPAA Security Regulations
2. NIST
3. SANS

Chief Executive Officer Date 8.21.15

Chair, Board of Directors Date 8-10-15

Date first adopted	6/24/2015 QI Committee	
Date revised		
New date adopted	7/13/2015	