



VIRTUAL PRIVATE NETWORK ACCESS USER SECURITY GUIDELINES THIRD PARTY USERS

These Guidelines apply to all usage of the Boise Cascade Company Virtual Private Network (“BC VPN”). All Vendors, Contractors and other third parties who are granted access to the BC VPN shall abide by these guidelines at risk of loss of access, termination of the service contract or both.

1. Use of the BC VPN service in the performance of activities unrelated to Contractor’s work for Boise Cascade is strictly prohibited, including incidental personal use of Boise Cascade’s network and IT resources, and use of any Boise Cascade resource for illegal conduct, or conduct that infringes the intellectual property rights of any third party.
2. Contractors authorized to access Boise Cascade’s network will be authenticated through their Boise Cascade network User ID and password. Contractors shall safeguard their VPN access as well as its components (software/security token, if any) from any unauthorized use, and shall prevent unauthorized access to Boise Cascade’s network from any VPN-connected computer.
3. When remotely connected to Boise Cascade’s network via VPN, Contractors shall adhere to the same Boise Cascade rules and regulations that apply to on-site usage, including Boise Cascade’s policies.
4. Contractors must be physically present at the console of the computer, and shall disconnect an active VPN connection when away from their computer or Contractor shall secure the computer so as to prevent unauthorized access to Boise Cascade’s network.
5. To use VPN client software, computers must meet Boise Cascade’s network configuration standards for machine hardware and VPN minimum requirements. Further, all computers connected to Boise Cascade’s network must:
 - a. Use a market-leading anti-virus protection with the latest updates and signature files installed.
 - b. Remain updated with the latest critical operating systems patches.
 - c. Use compatible firewall protection.

Computers that do not comply with these requirements or are found to be infected with viruses or worms will be disconnected from Boise Cascade’s systems. Boise Cascade shall not be responsible for any data loss or other damage that might result from such disconnection.

6. Contractor shall not bridge Boise Cascade’s network to another network using this VPN connection.
7. Data collected, stored, backed up, processed or accessed using this service must be protected according to Boise Cascade’s policies and procedures, including the privacy and confidentiality of any Boise Cascade data that has been accessed.
8. Contractor shall promptly return or destroy any Boise Cascade data in its possession immediately upon cessation of VPN service.
9. Contractor will not share or disclose any Boise Cascade data with any third party.
10. Contractors are required to register with Boise’s DUO multi-factor authentication application in order to access the Boise VPN. An iOS or Android device can be registered for push notifications, mobile numbers for SMS or land line numbers for call back.
11. In consideration of Contractor’s providing services to Boise Cascade, Contractor shall indemnify Boise Cascade from any violations of these requirements, including without limitation liability or claims related to third-party intellectual property or any data breach.