UC Santa Cruz Genomics Institute Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access OpenVPN Virtual Private Network (VPN) connections to the UC Santa Cruz Genomics Institute (GI) internal protected networks.

2.0 Scope

This policy applies to all GI employees, contractors, consultants, collaborators, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access GI networks.

3.0 Policy

Approved GI employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, 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, and paying associated fees.

Additionally:

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to GI internal networks.
2. VPN use is to be controlled using both password authentication and a public/private key system (one unique key per user).
3. When actively connected to the secure network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by GI network operational groups.
6. All computers connected to GI internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is available; this includes personal computers not owned by the GI.
7. Users of computers that are not GI-owned equipment must configure the equipment to comply with the GI's VPN and Network policies set forth in this document.
8. Only GI-approved VPN clients may be used.
9. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the GI's network, and as such are subject to the same rules and regulations that apply to GI-owned equipment, i.e., their machines must be configured to comply with the Security Policies of GI and the UCSC School of Engineering.
10. The user understands that the security of the private network the VPN allows access to is only as secure as the workstation or laptop the user is coming in from. Do not leave your workstation or laptop unattended while you are connected to the GI private networks via VPN, and regularly patch your workstation or laptop as patches are released from your OS vendor.
11. The user understands that they are being granted access to private and sensitive data, and as such the user agrees to not distribute the data in any way, in accordance with the guidelines set forth by the agencies that the data originated from.
12. The user must submit a National Institutes of Health (NIH) Computer Security Course Certificate to the GI IT staff prior to gaining VPN access.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and/or termination of involvement with any and all GI based projects.

I, the undersigned, have read, understand and agree to abide by the above VPN policies:

Name (Please Print) :____

Signature :____ Date:____________

Authorizing GI IT Staff Signature :____ Date:____________