CITY OF SAN RAFAEL

Virtual Private Network Service Agreement

I. Purpose

This document outlines an agreement for accessing the City of San Rafael's computer network by means of a Virtual Private Network (VPN) connection, within the Computer Use and Security Policy of the City. Remote access to the City network will be appropriately provisioned and/or controlled to ensure required security.

II. Definitions

Virtual Private Network (VPN): A VPN creates a secure connection, called a tunnel, between a client computer and a VPN server or host. This connection is usually made over the Internet and, in that case, has the effect of extending the City of San Rafael network to remote users. Once connected, a user may access files and/or applications stored on central servers just as if the user's machine was connected directly to the City Network at a City facility.

III. Service Terms and Conditions

Approved employees, contractors, and consultants may connect to the City Network via VPN. Approvals must be obtained from the appropriate management at the Department Director level and above as well as the City Information Technology (IT) Manager. Requestors must have a demonstrated business need to connect securely and/or to appear as a part of the City Network. Use of this service in the performance of activities unrelated to the mission of the City is strictly prohibited. VPN is a user managed service. As a result users of this technology are responsible for selecting an Internet Service Provider (ISP), coordinating installation with their ISP of any required software, and paying associated fees.

Additionally,

1. It is the responsibility of those with VPN privileges to prevent unauthorized access to the City Network from their VPN connected computer.
2. Users will be authenticated through their assigned City Network username and password.
3. Users with VPN privileges may only use VPN client software obtained or approved by the City's IT Division.
4. City Employees may only utilize the VPN client from a City assigned and configured computer.
5. All computers connected to City Network **must**:
    a. Use the most current anti-virus protection
    b. Keep computers updated with the latest critical operating systems patches
    c. Use compatible firewall protection.
6. When remotely connected to the City Network via VPN, users agree that they are subject to the same City rules and regulations that apply to on-site usage. In particular, users must adhere to the City of San Rafael Computer Use and Security Policy.
7. All requestors must read and agree to these terms and conditions before a connection is granted.
8. Data collected, stored, backed up, processed or accessed using this service must be protected according to City policies and procedures.
9. Proper data removal/destruction procedure must be followed for off-site systems at the end of employment, any contractual arrangement, or cessation of the individuals VPN service.

IV. Enforcement

All individuals granted access to this VPN service must adhere to the service terms and conditions. If these terms and conditions are violated, VPN access will be revoked. Violations will also be reported to the users' management, which may lead to other disciplinary action up to and including legal action and/or termination.

V. Request for authorization

I have read and agree to the terms and conditions stated above.

Requestor's Signature _____Signature Date_____

Printed Name_____ Title_____

Department or Company Name_____

Email Address_____ Daytime Phone_____

VI. Approval (INTERNAL USE ONLY)

Dept Director (or designee)_____Signature Date_____

Printed Name_____ Title_____

Effective Date_____ End Date (if known)_____

IT Manager (or designee)_____ _____Signature Date_____

Printed Name_____

VPN Granted Date_____ Terminated Date_____