Remote Consulting Group
1234 Main Street
Philadelphia, PA 19000-1213
www.rcg.com

Remote Access Policy

1. Overview

Remote Access allows Remote Consulting Group (RCG) to leverage the Internet to expand its physical network topology beyond its walls. This network expansion allows employees to access critical and sensitive business information from anywhere and at any time. Providing the ability to access business information remotely increases employee efficiency, but also presents risks to RCG's sensitive information, systems, and data.

2. Purpose

The purpose of this policy is to set standards and controls in place to protect RCG's systems, data, and information from the risks associated with remote access to its internal network over the Internet.

3. Scope

This policy applies to all RCG employees, contractors, vendors, suppliers, distributors, and any other third party entities that come into contact with an RCG owned computer, an RCG owned computing device, personally owned computer, or personally owned computing device used to remotely access RCG's network. This policy applies to any remote access connection used to access RCG's network, intranet, extranet, email system, database, and applications. This policy applies to any and all technical implementations of remote access used to access RCG's networks.

4. Policy

It is the responsibility of RCG's employees, contractors, vendors, suppliers, distributors, and any other third party entities with remote access privileges to RCG's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to RCG.

General access to the Internet through the RCG network is strictly limited to RCG employees, contractors, vendors, suppliers, distributors, and any other third party entities (hereafter referred to as "Authorized Users"). When accessing the RCG network from a personal computer, or computing device, Authorized Users are responsible for preventing access to any RCG computer resources or data by non-Authorized Users. Performance of

illegal or unauthorized activities through the RCG network by any (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information, see the *Acceptable Use* policy.

Authorized Users will not use RCG networks to access the Internet for outside business interests.

For additional information regarding RCG's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (www.rcg.com/RAS).

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e. Virtual Private Networks (VPNs)), strong passwords, and two-factor authentication. For further information, see the *Encryption Policy* and *Password Policy*.

4.1.2 Authorized Users shall protect their login and password, even from family members. For further information, see the *Password Policy*.

4.1.3 Two-Factor authentication must be used with VPN access. Acceptable forms of two-factor authentications are RSA SecurID hard token or Smart Cards/Badge. For further information on how the user can receive and register a hard token for remote access, see the *Remote Access Token Policy.*

4.1.4 Remote access communications applications other than those approved and identified in the table below may be used only if the applications are approved by the Information Security Department.

- PulseSecure
- RCG EVPN Client

4.1.5 Non-standard remote access communication devices must be reviewed and approved by Information Security Department before they are used to connect to RCG network and computing and information resources.

4.1.6 Remote access communication for suppliers to perform maintenance support on applications, hardware or operating systems programs, any password(s) required to access the application or systems programs must be given to the supplier only when

connectivity is established and immediately changed after each communication.

4.1.7 While using a RCG-owned computer, or computing device, to remotely connect to RCG's network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party entity.

4.1.8 Dual connectivity, such as establishing an outbound model call while simultaneously connected to the RCG intranet from a remote location, is prohibited.

4.1.9 Use of external resources to conduct RCG business must be approved in advance by the Information Security Department and the appropriate business unit manager.

4.1.10 All hosts that are connected to RCG internal networks via remote access technologies must use the most up-to-date anti-virus software (www.rcg.com/anti-virus_software), this includes personal computers and computing devices. Third party connections must comply with requirements as stated in the *Third Party Agreement Policy*.

4.1.11 Personal equipment used to connect to RCG's networks must meet the requirements of RCG-owned equipment for remote access as stated in the *Virtual Private Network (VPN)/Remote Access to RCG Networks Hardware and Software Policy*.

4.1.12 Information Security Department must ensure that remote access usage (e.g., reports and logs) are appropriately monitored.

4.1.13 No authorized user is to use Internet access through company networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.

4.1.14 All remote access connections must include a "time-out" system. In accordance with RCG's security policies, remote access sessions will timeout after 1 hour of inactivity, and will terminate after 12 hours of continuous connection. Both timeouts will require the user to reconnect and re-authenticate in order to re-enter company networks.

4.1.15 If a personally- or company-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and the Office of Information Systems immediately.

4.1.16 The remote access user also agrees to immediately report to their manager and the Office of Information Systems any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

4.1.17 All employees, suppliers, distributors, and other third parties that requires remote access to RCG network must complete an annual Cyber Awareness training within the last 12 months. Information Security Department will provide, monitor, and validate training requirements prior to approving remote access to users.

5. Policy Compliance

5.1 Compliance Measurement

The Information Security Department will verify compliance to this policy through various control methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection of RCG-owned computers, RCG-owned computing devices, personally owned computers, and personally owned computing devices.

5.2 Exceptions

Any exception to the policy must be approved by the Information Security Department and appropriate business unit manager in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any Third Party entity applicable to this policy and found to have violated this policy may be subject to legal action as set forth in the *Third Party Agreement Policy*.

6. Definitions

Terms	Definition

Remote Access	The ability to get access to a computer or a network from a remote distance
Third Party	Individuals, groups, or organization that provides product or services to RCG but are not directly employed by RCG.
Intranet	Secure and private enterprise network used to share data, computing, and other computer resources within RCG.
Extranet	Restricted network of computers that allows controlled access to a RCG's internal information to authorized outsiders (customers, suppliers, joint venture partners, etc.) by connecting them (usually via Internet) to the RCG's intranet.
Two-Factor Authentication	Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized, such as a username and password.
Virtual Private Network (VPN)	Is a technology that creates an encrypted connection over a less secure network, like the internet.
Dual Tunneling	Also known as split-tunneling. Simultaneous direct access to a non-RCG network (such as the internet, or a home network) from a remote device while connected to RCG's corporate network via a VPN tunnel.

7. Related Standards, Policies, and Processes

The following policies are applicable to protecting RCG's information and system assets when connecting via remote access and should be reviewed:

- Acceptable Use Policy
- Encryption Policy
- Password Policy
- Personal Identifiable Information (PII) Policy
- Data Classification and Handling Policy
- Third Party Agreement Policy
- Bring Your Own Device (BYOD)/Mobile Device Management (MDM) Policy
- Virtual Private Network (VPN)/Remote Access to RCG Networks Hardware and Software Policy
- Remote Access Token Policy

8. Revision History

Date of Change	Responsible	Summary of Change Rev #	Approved By/Date
13 Oct 2016	Information Security	Initial Policy/Ver 1.0	S.D. Winchester, CIO 14 Oct 2016