Please note that this sample policy is provided only as an example and is for reference purposes only. In many instances, your existing policies and procedures may suffice. Prior to developing a policy or adopting this sample policy, Century Business Technologies strongly encourages any organization to consult with its legal counsel, accounting, financial and/or human resource professionals. By doing so, this will assist your organization in developing policies and procedures that reflect its organizational philosophy and that are appropriate to their specific circumstances and that are consistent with applicable federal, state and local laws. This is provided as a free resource and is provided "as is" without warranty of any kind and Century Business Technologies makes no legal representation concerning the adequacy of this policy or its compliance with federal, state or local laws. Never use sample policies and procedures that you find online as-is, as any policy you adopt needs to reflect the actual practices in your company. They must also be in compliance with all applicable laws and regulations, and there can be significant differences in state and local compliance requirements. You should always consult with a licensed attorney with experience specific to employment law prior to finalizing policies and procedures, whether they are individual documents or combined to form an employee handbook or procedures manual.

1.0 Purpose

The purpose of this policy is to define standards for connecting to _____ network from any host. These standards are designed to minimize the potential exposure to _____ from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

2.0 Scope

This policy applies to all _____ employees, contractors, vendors and agents with a company-owned or personally-owned computer or workstation used to connect to the _____ network. This policy applies to remote access connections used to do work on behalf of _____, 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, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

3.0 Policy

3.1 General

1. It is the responsibility of _____ employees, contractors, vendors and agents with remote access privileges to _____'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
2. General access to the Internet for recreational use by immediate household family on personal computers that have access to the _____ network is permitted. The employee is responsible to ensure the family member does not violate any policies, does not perform illegal activities, and does not access to the company network unless supervised by the employee. The employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of _____'s network:
    a. *Acceptable Encryption Policy*
    b. *Wireless Communications Policy*
    c. *Acceptable Use Policy*

3.2 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. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any _____ employee provide their login or email password to anyone, not even family members.
3. _____ employees and contractors with remote access privileges must ensure that their company-owned or personal computer or workstation, which is remotely connected to _____'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. _____ employees and contractors with remote access privileges to _____'s corporate network must not use non-company email accounts (i.e., Outlook, Yahoo, G-Mail), or other external resources to conduct company business, thereby ensuring that official business is never confused with personal business. polic
5. Reconfiguration of a home user'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 _____, and the CTO must approve security configurations for access to hardware.
7. All hosts that are connected to _____ internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in their agreement.
8. Personal equipment that is used to connect to _____'s networks must meet the requirements of company-owned equipment for remote 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.

5.0 Definitions

Term	**Definition**
Cable Modem	Cable companies such as Cox & AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and connecting into another Internet service provider (ISP). Being on a Company-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into _____ and an ISP, depending on packet destination.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

ISDN There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to _____'s corporate network through a non-_____ controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-_____ network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into _____'s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Date of Change	Responsible	Summary of Change
03/03/2020		

1. Customize the Policy to Fit All of the Client Needs

The policy you help create should be customized to not only legally protect the employer and employee rights, but it needs to reflect the capabilities of the corporate infrastructure. Take VPNs and firewalls, for example:

- If a good firewall is in place with adequate VPN licenses, has it been configured correctly?
- Do the users already know how to install the VPN and connect, or do step-by-step instructions need to be provided?
- Do additional VPN licenses need to be procured and provisioned to accommodate the larger than normal remote workforce?

2. Make the Policy Easy to Understand

The policy you help put in place for remote workers needs to be understandable and taught correctly to the entire workforce. Clear and concise instructions will help the new process go smoothly. To ensure everyone understands what they need to do and what is expected of them, we suggest a webinar or in-person training to explain why the policy is in place.

It's common sense that people won't take actions that slow down their tasks if they don't have an emotional buy-in to the importance of following the policy. You need to change their behavior. Explain why the policy is in place, what is at stake for the company if the policy isn't followed, and importantly, how they will benefit from following the policy.

When this particular policy is taught, we recommend it includes information on tips to protect their home network. This makes them consider how they are protecting themselves and their family to cyberthreats, and will, in turn, lead to a better, more secure environment for the company. It's a win-win.

3. Have Employees Sign the Policy for Acceptance and Compliance

After you have created the policy, presented it to the employees, and have buy-in from the staff, pass the final policy off to employees to sign and acknowledge they understand what's in the policy. This lets you know the employees have read the policy, they accept what is in it, and shows you're complying to any standards or regulations.

Simplifying the Training

We've made the training part of creating a remote workforce policy as easy as possible. We're offering a template for a training presentation, based on a hypothetical company, for you to customize for any business. You can use this template with updated Remote Worker Policy text included on the final pages to teach this important information to your clients.

We hope these tips and template will help you be proactive in education and security for your clients' businesses and their remote workforce. Don't forget to communicate the measures you're taking as a TSP to continue to serve your clients when your staff may be working remotely for an extended period.

We're all in this together.