1. Purpose

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

2. Scope

This policy applies to all People employees, contractors, vendors and agents with a People-owned or personally-owned computer or workstation used to connect to the People network. This policy applies to remote access connections used to do work on behalf of People, 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 DSL, VPN, SSH.

3. Policy

It is the responsibility of People employees, contractors, vendors and agents with remote access privileges to People's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to People.

General access to the Internet for recreational use by immediate household members through the People Network on personal computers is permitted. The People employee is responsible to ensure the family member does not violate any People policies, does not perform illegal activities, and does not use the access for outside business interests. The People employee bears responsibility for the consequences should the access be misused.

4.1 Requirements

4.1.1 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*.

4.1.2 At no time should any People employee provide their login or email password to anyone, not even family members.

4.1.3 People employees and contractors with remote access privileges must ensure that their People-owned or personal computer or workstation, which is remotely connected to People'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.

4.1.4 People employees and contractors with remote access privileges to People's corporate network must not use non-People email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct People business, thereby ensuring that official business is never confused with personal business.

4.1.5 Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

4.1.6 Non-standard hardware configurations must be approved by Remote Access Services, and People must approve security configurations for access to hardware.

4.1.7 All hosts that are connected to People internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

4.1.8 Personal equipment that is used to connect to People's networks must meet the requirements of People-owned equipment for remote access.

4.1.9 Organizations or individuals who wish to implement non-standard Remote Access solutions to the People production network must obtain prior approval from Remote Access Services and People.

4. Policy Compliance

5.1 Compliance Measurement

The People Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the People Security Team 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.

6 Revision History

Date of Change	Responsible	Summary of Change
June 2014	Sat Sindhar	Introduced Policy.