1. Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the People network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on People computer systems.

2. Purpose

This policy defines the requirements for remote access tools used at People

3. Scope

This policy applies to all remote access where either end of the communication terminates at a People computer asset

4. Policy

All remote access tools used to communicate between People assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools

People may provide mechanisms to collaborate between internal users, with external partners, and from non-People systems. The approved software list is:

Skype
Webex
JoinME
Windows RDP

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

a) All remote access tools or systems that allow communication to People resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
b) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the People network encryption protocols policy.
c) All People antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard People procurement process, and the information technology group must approve the purchase.

5. 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