

IBS - TeamViewer -- Remote Access Policy

v2008_09_23.01

1.0 Purpose

The purpose of this policy is to define standards for connecting to client network from any host using TeamViewer. These standards are designed to minimize the potential exposure to our client from damages that may result from unauthorized use of 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 Innovative Business Systems, Inc. employees, owned or personally-owned computers or workstations used to connect. This policy applies to remote access connections used to do work on behalf of “IBS” clients including routine maintenance and network administration.

Remote access implementations that are covered by this policy include access provided by TeamViewer. Other remote access tools are not approved, unless authorized by IBS management and/or the “IBS” client for whom remote access is being engaged.

3.0 Policy

3.1 General

1. It is the responsibility of “IBS” employees with remote access privileges to ensure that their remote access connection is given the same consideration as the user’s on-site connection to that client.
2. General access to the Internet through the remote access connection are subject to the same company policies that would apply on site and “IBS” employees are responsible to ensure their remote access connection isn’t used to perform illegal

activities, and that access is not used for outside business interests. 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 client networks via remote access methods.

a. IBS Encryption Policy

4. For additional information regarding to use to TeamViewer to gain remote access to client networks including how to connect and disconnect service, troubleshooting, etc., go to the see the “TeamViewer Security Statement”.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via a one-time unique session ID along with password authentication.

2. Employees with remote access privileges must ensure that their owned or personal computer or workstation, which is remotely connected to client’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.

3. All hosts that are connected to customer internal networks via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.

4. Personal equipment that is used to connect to customer’s networks must meet the requirements of that customers own equipment for remote access.

5. Organizations or individuals who wish to implement non-standard Remote Access solutions to the customer’s production network must obtain prior approval from that customer before connecting whether the connection is made by a conventional TeamViewer connection or a Host-Mode connection.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.