

---

# Security Provisions for

Remote Computer Operations

## **Ensuring Data Security for Remote Computer Operations**

**White Paper**

---

**Abstract**

We are very conscious of data security. We've been doing it since 1986 without a breach.

© 2007 by Bill Good Marketing, Inc.

*This information represents the current view of the author as of the date of publication. Because of the rate at which conditions are changing, the author reserves the right to alter and update his opinion based on new conditions.*

*This White Paper is for informational purposes only. Copyright permission is hereby granted to make copies and distribute to Registered Representatives in the United States and Canada.*

*Bill Good  
Chairman*

*Bill Good Marketing, Inc.  
12393 Gateway Park Place, Ste 600  
Draper, UT 84020  
800-678-1480 · 801-572-1480*

---

CONTENTS

Security Provisions for Remote Computer Operations i

ENSURING DATA SECURITY FOR REMOTE COMPUTER OPERATIONS ..... I

WHITE PAPER..... I

CONTENTS .....III

TWO NEW SERVICES ..... 1

Emergency Computer Operator Service 1

Permanent BGM CO 1

HOW IT WORKS ..... 2

DATA ENCRYPTION..... 3

PREVENTING UNAUTHORIZED ACCESS..... 4

Inactivity Access Code Prompt: 4

Prominent Notification When Computer Is Being Accessed 4

Notification of Last Access 4

Log of Sessions 4

Time Restrictions 5

COMPUTER SECURITY ..... 6

Multiple, Nested Passwords 6

Limited Number of Log-In Attempts 6

ADDITIONAL SECURITY ..... 7

Internet Security 7

PHYSICAL SECURITY ..... 8

DOCUMENT SECURITY..... 9

---

|                              |    |
|------------------------------|----|
| Paper/Hard Copy Security     | 9  |
| Electronic Document Security | 9  |
| SERVICE SET-UP .....         | 10 |

---

---

## TWO NEW SERVICES

### Emergency Computer Operator Service

If you lose your CO, we can take over your computer operations as early as tomorrow, assuming you are properly set up. And we will stay as long as you want but with the understanding that the minimum job we will take is 2 weeks.

### Permanent BGM CO

We do all your computer operations for you—remotely. You will have your own CO at our location. You can communicate with him or her in a variety of ways (See, “How It Works,” Page 2.)

Every day, your CO will perform all the steps from the CO Daily Task Checklist that apply to you. On Friday, or another day that you designate, your CO will perform the end of week tasks.

Twice a month, your CO will perform required system maintenance, and once a month, will produce all the necessary reports for your monthly planning meeting.

---

## HOW IT WORKS

To access your computer, we will be using a business edition of GoToMyPC. You may have heard the ads for this. If you signed up for it individually, you could get on your own computer remotely from any Internet-connected computer in the world.

We are satisfied with its security protocols.

GoToMyPC uses several methods to help prevent unauthorized access to your computer. BGM will not give usernames and passwords to any user who is not authorized to access your data.

---

## DATA ENCRYPTION

GoToMyPC has Advanced Encryption Standard (AES) encryption built in. All data including screen images, keyboard and mouse input and chat text is fully encrypted from end to end. The encryption key is unique for each connection and is based on the PC's access code and a random bit sequence. The access code itself resides on the host computer and is never transmitted or stored on Citrix Online servers. For this reason, it is impossible, even with the most sophisticated devices, to intercept the data necessary to decode the encryption. Transmissions cannot be hacked or compromised in any way.

---

## PREVENTING UNAUTHORIZED ACCESS

GoToMyPC uses several methods to help prevent unauthorized access to your computer.

All COs will be required to have strong passwords; 8 characters in length, minimum, and must use a combination of numbers and letters. The Manager will make sure passwords are stored in a secure location.

Passwords will be changed every 90 days unless a new CO is assigned to your account.

If a CO leaves or is replaced, that user will have their network access immediately terminated and all GoToMyPC rights will be removed.

### Inactivity Access Code Prompt:

After a set period of inactivity your CO must reauthenticate to the remote session using the secure authentication code.

### Prominent Notification When Computer Is Being Accessed

Whenever a computer running GoToMyPC is accessed remotely, a notice will appear on the screen. This prevents unauthorized parties from connecting to your computer without you being aware of it.

### Notification of Last Access

Your CO will receive a notification of the last time your computer was accessed each time they access your computer.

### Log of Sessions

Bill Good Marketing will have access to a log of all remote access sessions and will verify that no unauthorized sessions have occurred

---

## Time Restrictions

BGM will implement time restrictions based on approved times that we will take remote control of your computer.

Only one user and one computer at a time will be allowed remote access into your office.

---

## COMPUTER SECURITY

From our location there will be only one designated workstation that will be set up to access your computer. With the tightened security features of GoToMyPC, your computer cannot be accessed from any other workstation or location.

### Multiple, Nested Passwords

The CO must first log in to the secure website using the designated email address and password for his/her computer.

Then, when he/she selects your computer, he/she must enter a second password—the computer's unique access code—to complete the connection. An access code is required for all connections.

GoToMyPC requires that passwords be at least 8 characters long and contain both letters and numbers. These strict requirements protect you from using easily compromised or common passwords.

### Limited Number of Log-In Attempts

To protect against hacker attacks, GoToMyPC limits the number of logon attempts.

---

## ADDITIONAL SECURITY

Computer and Users will be attached to a secure Microsoft Active Directory server that is behind two locked doors. Only authorized users will be given access to log on to the CO machines. Only IT administrators have access to the server room.

All USB devices, writeable CD drives, or other external devices will be disabled on the computers used by BGM staff in servicing your account.

Current Virus scanning software will be installed and kept up to date on all CO machines.

Current Spyware scanning software will be installed and kept up to date on all CO machines.

BGM will verify that all appropriate security patches are installed on the local computer for all applicable software.

Screen captures will not be allowed.

### Internet Security

All Internet traffic will be filtered by a corporate firewall. Additionally, your CO will only be allowed to travel to approved websites, e.g. <http://www.billgood.com>.

---

## PHYSICAL SECURITY

The Remote Computer Operations will be performed in a confined area and only authorized individuals be allowed to use any equipment in that area. We will also have a security camera(s) covering the entire area where computer operations will be performed.

A Manager will be on-site during all work hours. This person will also help regulate physical access to this area.

---

## DOCUMENT SECURITY

### Paper/Hard Copy Security

You may have a need to send us documentation about your clients via fax/mail. Obviously, this generates paper copies of your data that you are not in control of. When your CO receives documentation it will be placed in a folder with your name on it. This folder will be placed in a locked file cabinet until your CO can perform the necessary data entry. The folder will be immediately put back in the locked cabinet until a Manager verifies the procedures have been completed as desired. At which point, the Manager will shred the documentation in a cross-cut shredder. The only documentation we will keep is documentation attesting that the work has been completed as desired.

### Electronic Document Security

You may choose to send us paperwork electronically, either through email or some other method, such as CopyTalk<sup>®</sup>. BGM uses GroupWise 7 as its email solution and has found it to be a very secure and reliable solution. Our email server sits behind two firewalls; one firewall is a general purpose firewall and the other specifically filters SPAM, viruses and potentially unsafe attachments.

A Manager will spot-check all emails sent by COs to verify no unauthorized data is being sent.

Electronic files that are received in other ways will be securely deleted after your CO performs the appropriate action that handles the needs of the document. BGM will not keep any copies of this electronic data.

---

## SERVICE SET-UP

In order to properly service your account, several things must occur.

- 1) You will need to represent to BGM that you have received compliance approval for this program and signed the proper service agreement.
- 2) We need to run the *New Client Procedure Checklist* to ensure that the GoToMyPC software is installed and set up on the computer in your office.
- 3) We need a data sheet on who is who and what peculiarities your office may have that we need to consider.
- 4) We need to conduct a briefing with your entire staff so they know what to expect and very importantly know how to communicate with us.
- 5) We'll make a test of the connection from our office to yours.
- 6) We will print a test letter.

Then we're ready to go to work for you.