Collaboration User Agreement & Information Security Awareness Training:

1. *Read this section to understand your responsibilities.*
2. *Direct any questions to your Clearpoint Business Group Sponsor.*
3. *Acknowledge your understanding of your responsibilities by completing and signing the acknowledgement at the end of this document. Return the acknowledgement to your Clearpoint Business Group sponsor as directed at the end of this document.*

Introduction

As a contractor, supplier or partner of Clearpoint Business Group, you have a responsibility to safeguard the information in accordance with applicable contracts, non-disclosure agreements, proprietary information agreements, as well as Clearpoint Business Group information security requirements. Every individual with access to Clearpoint Business Group computing or information resources must follow relevant information protection requirements, maintain the integrity of Clearpoint Business Group resources and protect them from unauthorized access.

Access to Clearpoint Business Group computing and information resources is granted only to authorized individuals and is restricted to only what is required based on citizenship, job function, need-to-know, employment status and management approval.

Clearpoint Business Group computing and information resources may only be used for Clearpoint Business Group business purposes and for no other reason.
The following areas of information protection must be observed by Clearpoint Business Group trading partners:

- User ID and password controls for information and computing resources
- Conditions and responsibilities
- Identifying and protecting sensitive information
- Remote access
- Protection from virus and other malicious code/logic
- Workstation security
- Network security
- Lync Services
- Public Key Infrastructure (PKI)

1. User ID and Password Controls

The password is the most critical line of defense in protecting computing and information resources. Each individual with approved access to Clearpoint Business Group computing and information resources is responsible for maintaining original, unique and strong passwords.

1. Create passwords consisting of at least 12 characters containing numbers, letters, and special characters where possible.
2. Change passwords periodically. Passwords will expire after 90 days and must be changed prior to expiration.
3. Change passwords immediately if compromised in any way.
4. Keep passwords secret and do not write them down or openly display them. If you need to write them down, store them securely.
5. Create a strong password that is easy for you to remember, but hard for someone else to guess. Avoid nicknames, family names, pet names, hobbies and car license or telephone numbers.
6. Be careful when typing in your password that no one is looking over your shoulder.
7. Never share your password, user ID or other access information.
8. Shared or group accounts shall not be permitted.

2. Conditions and Responsibilities

The following banner statement will be presented at login to notify and advise the user of the conditions and responsibilities associated with accessing Clearpoint Business Group information and computing resources. Each user must accept these terms prior to being permitted access to any Clearpoint Business Group computing or information resources.

This computer system is the property of Clearpoint Business Group, LLC. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, the Company's Acceptable Use of Information Technology Resources Policy ("AUP"). Users have no expectation of privacy (except where such an expectation is established under local law). Regardless of where you are located you understand that third parties may monitor and review user activity, including files and e-mails, and may transfer this information to the United States for processing. Unauthorized use of this system is prohibited and may result in denial of access, disciplinary action and/or legal action. Information transmitted to a foreign person on this network may be subject to applicable Export Control laws.

(Note: alternate versions of this banner may exist in accordance with ITS Policy 700-11)

3. Identifying and Protecting Sensitive Information

"Sensitive information" refers to any data (written, pictorial, electronic, audio, oral or other form) qualifying as Clearpoint Business Group proprietary, third party proprietary, or subject to export control regulations. Sensitive information must be appropriately identified and protected through required means such as labeling, encryption, access controls, approved authentication methods, strong passwords and accountability measures.

Failure to comply with sensitive information controls not only violates Clearpoint Business Group policy, but also may lead to a violation of law, large fines and jail terms for the individual responsible for failing to protect sensitive information from exposure. Know the sensitivity of the information to which you have access, what controls are in place and protect it accordingly.

3.1 Sensitive Information Labeling Requirements

All sensitive information must bear the required labels to indicate the sensitivity. These labels or markings must be readily visible to identify the information using one or more of the following three labels as appropriate:

- "Clearpoint Business Group Confidential & Proprietary Information" (may be abbreviated "CBG Confidential" or "CBG Proprietary" but never "CCPI")
- "Third Party Proprietary Information"
- "Export Controlled Information"

The following are examples of how to apply the appropriate labels to various media that may contain sensitive information:

- **Printed material**: Label must be visible at the top or bottom of each page.
- **E-mail**: Label must appear in the subject line.
- **Web pages**: Label must appear clearly at either the top or bottom of each page displaying sensitive information.
- **Faxes**: Cover sheet must identify the sensitivity of the information. Also, the remaining pages must follow the same labeling requirements of other printed sensitive information.
- **CD-ROMS, DVDs, floppy disks, and other computer media**: Label must appear on all media containing sensitive information, such as the case and/or face of a CD-ROM, label on a floppy disk, etc. Documents contained on labeled media must still bear the required sensitivity label, even though the medium is labeled.

3.2 Storing or Disposing of Sensitive Information

Sensitive information in hard copy form or on portable electronic media must be secured in a locked desk, locked office, or locked cabinet or container. Sensitive information in hard copy form should be placed in a secure container designated for disposal of sensitive information, or otherwise destroyed in a manner that precludes its reconstruction, such as shredding.

4. Remote Access

Remote access exposes a company's information to serious risks. Remote access to the Clearpoint Business Group Collaboration Extranet is controlled through the use of network security systems. Every individual with approved access to the Clearpoint Business Group Collaboration Extranet is responsible for proper use of the access and adhering to information protection guidelines and requirements.

5. Viruses and Malicious Code/Logic

A computer virus is an unwanted instruction or program designed and written to adversely affect your computer or the information you are accessing by altering the way that information or computer works without your permission. To minimize the risk of contracting a virus, Clearpoint Business Group requires up-to-date anti-virus software on every machine with access to the Clearpoint Business Group Collaboration Extranet.

Anti-Virus Software: User agrees to acquire, install, utilize, and maintain anti-virus software (McAfee VirusScan, Symantec AntiVirus Corporate Edition, or equivalent) on any computer system used to access the Clearpoint Business Group Federation Services applications. Clearpoint Business Group recommends scanning of all files on the computer system on a weekly basis (after hours is sufficient), checks for and deployment of new Anti-Virus signature files on a weekly basis, and checks for and deployment of new Anti-Virus engine files on a regular basis (based on the scan engine release schedule of the Anti-Virus application provider). Additional measures include:

- Saving and scanning attachments and downloaded files before opening them.
- Blocking or not opening risky file types (.exe, .bat, .vbs, .scr).
- Running full disk virus scan on a regular basis. Clearpoint Business Group recommends weekly scanning.

6. Workstation Security

Never leave your workstation unsecured. If you leave your work area, password lock or shut down the applications or system you are using. Screen saver lock-out time requirement is 30 minutes for standard accounts.

7. Network Security Measures

Network security holes can open a trading partner's network to attack, and thereby endanger Clearpoint Business Group information to which the partner has access.

- Prohibit desktop modems with auto-answer capability.
- Protect wiring closets and deactivate wiring drops in areas under construction.
- Disable all unnecessary programs and functions on computer systems.
- Disable accounts without passwords or default passwords.
- Promptly delete accounts when users leave or change job responsibilities.

8. Lync Services

Lync Services conducts real-time meetings and collaboration sessions through the Corporate Internet firewall, facilitating virtual data exchange between internal Clearpoint Business Group users as well as partners, customers and suppliers outside of the Clearpoint Business Group Intranet. Therefore, any information shared using Lync Services must follow the sensitive information protection guidelines and Clearpoint Business Group proprietary requirements.

8.1 Properly Identify Lync Services Users

To ensure that the virtual conference is compliant, the meeting participants and their proper level of access must be recognized and any shared information needs to be properly identified and

labeled. When hosting a Lync Services session, it is the host's responsibility to identify and recognize all conference participants.

Lync Services provides the ability to authenticate to a meeting in which sensitive, proprietary or export controlled data will be exchanged. To authenticate to such a meeting you will need an account. A meeting host may deny access to unauthenticated guests. If no sensitive information is being exchanged, you may be admitted to the meeting as an unauthenticated guest.

8.2. Use Caution When Sharing Control of an Application

Virtual conferencing is all about sharing displays of applications such as PowerPoint™, Word™, and Excel™, etc. In addition to sharing displays, the conferencing software also allows one to give control of a shared application to another meeting participant. **Please use caution when sharing control of an application**. If you give control of an application, always monitor the remote user's activities. If you notice unapproved activities such as use of the "File Open" command - immediately hit the "ESC" key to take away the remote control privilege. Handing off remote control of an application may give the person the ability to assume your identity and take complete control of your workstation and all attached network resources. If unsupervised control of the application is permitted, files could be deleted, malicious web sites could be visited and sensitive files could be retrieved from your workstation.

9. Public Key Infrastructure (PKI)

The Clearpoint Business Group enterprise Public Key Infrastructure (PKI) shall enable the protection of Clearpoint Business Group information and resources and facilitate secure electronic transactions through the issuance of digital certificates that enable public-key cryptography services. Additional information will be provided when you make your request to obtain a digital certificate following account creation.

Password-protect the certificate using a password with the characteristics described above in section 1, User ID and Password Controls. Don't share your private certificate. If at all possible, store the private certificate on a removable token. Don't store your private certificate on a public computer where others can access it. Don't store your certificate on Windows 9x computers where other users of the computer can easily obtain it.

10. Problem Reporting

The Clearpoint Business Group Service Desk is a centralized support organization within Clearpoint Business Group. If at any time you suspect inappropriate use of your account, misuse of the system or malicious code or virus infection, contact Clearpoint Business Group at one of the following phone numbers as soon as possible to report the event.

To contact the Clearpoint Business Group Service Desk, dial 1-888-602-8492 and choose the option for the ITS Helpdesk.