Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all Commercial Connect LLC employees and affiliates.

3.0 Policy

All Commercial Connect LLC encryption shall be done using NIST approved cryptographic modules. Common and recommended ciphers include AES 256, Triple DES and RSA. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Commercial Connect LLC's key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Version 1.1 October 11, 2010, require NIST approved products

Analog/ISDN Line Security Policy

Purpose

This document explains Commercial Connect LLC analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

2.0 Scope

This policy covers only those lines that are to be connected to a point inside Commercial Connect LLC building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-corporate information purposes.

3.0 Policy

3.1 Scenarios & Business Impact

There are two important scenarios that involve analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside Commercial Connect LLC premises, then there is the possibility of breaching Commercial Connect LLC's internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This potentially results in the loss of millions of dollars’ worth of corporate information.

The second scenario is the threat of anyone with physical access into a Commercial Connect LLC facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted networking of Commercial Connect LLC through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon Commercial Connect LLC information to an unknown location. This could also potentially result in the substantial loss of vital information.

Specific procedures for addressing the security risks inherent in each of these scenarios follow.

3.2 Facsimile Machines

As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.

- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.
- A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.

Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When in use, the computer is to be physically disconnected from Commercial Connect LLC's internal network.
- The line will be used solely for Commercial Connect LLC business, and not for personal reasons.
- All downloaded material, prior to being introduced into Commercial Connect LLC systems and networks, must have been scanned by an approved anti-virus utility (e.g., McAfee Virus Scan) which has been kept current through regular updates.

3.3 Computer-to-Analog Line Connections

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within Commercial Connect LLC will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to Commercial Connect LLC, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case by case basis.

Replacement lines, such as those requested because of a move, fall under the category of "new" lines. They will also be considered on a case by case basis.

3.4 Requesting an Analog/ISDN Line

Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Telecom:

- a clearly detailed business case of why other secure connections available at Commercial Connect LLC cannot be used,
- the business purpose for which the analog line is to be used,
- the software and hardware to be connected to the line and used across the line,
- and to what external connections the requester is seeking access.

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is a Commercial Connect LLC-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?
- Why is Commercial Connect LLC's current dial-out access pool unable to accomplish the same tasks as an analog line?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

- Will the machines that are using the analog lines be physically disconnected from Commercial Connect LLC's internal network?
- Where will the analog line be placed? A cubicle or lab?
- Is dial-in from outside of Commercial Connect LLC needed?
- How many lines are being requested, and how many people will use the line?
- How often will the line be used? Once a week, 2 hours per day...?
- What is the earliest date the line can be terminated from service?
- The line must be terminated as soon as it is no longer in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What types of protocols will be run over the line?
- Will a Commercial Connect LLC-authorized anti-virus scanner be installed on the machine(s) using the analog lines?
- The requester should use the Analog/ISDN Line Request Form to address these issues and submit a request.

4.0 Enforcement

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

5.0 Revision History

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with Commercial Connect LLC's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

Application Service Providers (ASP) Policy

1.0 Purpose

This document describes Information Security's requirements of Application Service Providers (ASPs) that engage with Commercial Connect LLC.

2.0 Scope

This policy applies to any use of Application Service Providers by Commercial Connect LLC, independent of where hosted.

3.0 Policy

3.1 Requirements of Project Sponsoring Organization

The ASP Sponsoring Organization must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within Commercial Connect LLC or ASPs external to the company. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this policy. The Business Function to be outsourced must be evaluated against the following:

1. The requester must go through the ASP engagement process with the ASP Tiger Team to ensure affected parties are properly engaged.
2. In the event that Commercial Connect LLC data or applications are to be manipulated by, or hosted at, an ASP's service, the ASP sponsoring organization must have written, explicit permission from the data/application owners. A copy of this permission must be provided to InfoSec.
3. The information to be hosted by an ASP must fall under the "Minimal" or "More Sensitive" categories. Information that falls under the "Most Sensitive" category may not be outsourced to an ASP. Refer to the *Information Sensitivity Policy* for additional details.
4. If the ASP provides confidential information to Commercial Connect LLC, the ASP sponsoring organization is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. Commercial Connect LLC's legal services department should be contacted for further guidance if questions about third-party data arise. Projects that do not meet these criteria may not be deployed to an ASP.

3.2 Requirements of the Application Service Provider

InfoSec has created an associated document, entitled *ASP Security Standards* that sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use.

The ASP engagement process includes an InfoSec evaluation of security requirements. The *ASP Security Standards* can be provided to ASPs that are either being considered for use by Commercial Connect LLC, or have already been selected for use.

InfoSec may request that additional security measures be implemented in addition to the measures stated in the *ASP Security Standards* document, depending on the nature of the project. InfoSec may change the requirements over time, and the ASP is expected to comply with these changes.

ASPs that do not meet these requirements may not be used for Commercial Connect LLC Systems, Inc. projects.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	**Definitions**
Application Service Provider (ASP)	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a Commercial Connect LLC-owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.
ASP Sponsoring Organization	The group within Commercial Connect LLC that wishes to utilize the services of an ASP.
Business Function	The business need that a software application satisfies. managed by an ASP that hosts an application on behalf of Commercial Connect LLC.

6.0 Revision History

Server Audit Policy

1.0 Purpose

The purpose of this policy is to ensure all servers deployed at Commercial Connect LLC are configured according to the Commercial Connect LLC security policies. Servers deployed at Commercial Connect LLC shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Ensure conformance to Commercial Connect LLC security policies

2.0 Scope

This policy covers all servers owned or operated by Commercial Connect LLC. This policy also covers any server present on Commercial Connect LLC premises, but which may not be owned or operated by Commercial Connect LLC.

3.0 Policy

Commercial Connect LLC hereby provides its consent to allow CAS-Com Internet Services, Inc. to access its servers to the extent necessary to allow <Audit organization> to perform scheduled and ad hoc audits of all servers at Commercial Connect LLC.

3.1 Specific Concerns

Servers in use for Commercial Connect LLC support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of these systems.

3.2 Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include:

- All system logs shall be sent to a central log review system
- All Sudo / Administrator actions must be logged
- Use a central patch deployment system
- Host security agent such as antivirus shall be installed and updated
- Network scan to verify only required network ports and network shares are in use
- Verify administrative group membership
- Conduct baselines when systems are deployed and upon significant system changes
- Changes to configuration template shall be coordinated with approval of change control board

3.2 Responsibility

CAS-Com Internet Services, Inc. shall conduct audits of all servers owned or operated by Commercial Connect LLC. Server and application owners are encouraged to also perform this work as needed.

3.4 Relevant Findings

All relevant findings discovered as a result of the audit shall be listed in the Commercial Connect LLC tracking system to ensure prompt resolution or appropriate mitigating controls.

3.4 Ownership of Audit Report

All results and findings generated by the CAS-Com Internet Services, Inc. Team must be provided to appropriate Commercial Connect LLC management within one week of project completion. This report will become the property of Commercial Connect LLC and be considered company confidential.

4.0 Enforcement

CAS-Com Internet Services, Inc. shall never use access required to perform server audits for any other purpose. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Automatically Forwarded Email Policy

1.0 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Commercial Connect LLC.

3.0 Policy

Employees must exercise utmost caution when sending any email from inside Commercial Connect LLC to an outside network. Unless approved by an employee's manager InfoSec, Commercial Connect LLC email will not be automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

4.0 Enforcement

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

5.0 Definitions

Terms	**Definitions**
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to Commercial Connect LLC or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

6.0 Revision History

Bluetooth Policy

1.0 Purpose

This policy provides for more secure Bluetooth Device operations. It protects the company from loss of Personally Identifiable Information (PII) and proprietary company data.

2.0 Scope

This policy covers all Commercial Connect LLC Bluetooth Devices.

3.0 Policy

3. 1Version level

No Bluetooth Device shall be deployed on Commercial Connect LLC equipment that does not meet Bluetooth v2.1 specifications without written authorization from the InfoSec Manager. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

3.2 Pins and Pairing

*When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area. If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, **you must refuse the pairing request and** report it to InfoSec, through your Help Desk, immediately. Unless your Bluetooth device itself has malfunctioned and lost its pin, this is a sign of a hack attempt.*

3.3 Device Security Settings

All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.

If your device allows the usage of long PIN's, you must use either a 13 alphabetic PIN or a 19 digit PIN (or longer).

Switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed.

Update the device's firmware when a new version is available.

3.4 Security Audits

InfoSec shall perform audits to ensure compliancy with this policy. In the process of performing such audits, InfoSec shall not eavesdrop on any phone conversation.

3.5 Unauthorized Use

The following is a list of unauthorized uses of Commercial Connect LLC-owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any for of attacking other Bluetooth enabled devices.
- Using Commercial Connect LLC-owned Bluetooth equipment on non-Commercial Connect LLC-owned Bluetooth enabled devices.
- Unauthorized modification of Bluetooth devices for any purpose.

3.6 User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth users must only access Commercial Connect LLC information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to InfoSec.

4.0 Enforcement

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

5.0 Definitions

Terms ***Definitions***

6.0 Revision History

Version	*Author*	*Update Comments*

Database Password Policy

1.0 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Commercial Connect LLC's networks.

Computer programs running on Commercial Connect LLC's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2.0 Scope

This policy applies to all software that will access a Commercial Connect LLC, multi-user production database.

3.0 Policy

3.1 General

In order to maintain the security of Commercial Connect LLC's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

3.2 Specific Requirements

3.2.1. Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.
- Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.

- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

3.2.2. Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

3.3. Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

3.4. Coding Techniques for implementing this policy

[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or Cpro.]

4.0 Enforcement

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

5.0 Definitions

Term	**Definition**
Computer language	A language used to generate programs.
Credentials	Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.

Executing body
The series of computer instructions that the computer executes to run a program.

Hash
An algorithmically generated number that identifies a datum or its location.

LDAP
Lightweight Directory Access Protocol, a set of protocols for accessing information directories.

Module
A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.

Name space
A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.

Production
Software that is being used for a purpose other than when software is being implemented or tested.

6.0 Revision History

Commercial Connect LLC Email Use Policy

1.0 Purpose

To prevent tarnishing the public image of Commercial Connect LLC When email goes out from Commercial Connect LLC the general public will tend to view that message as an official policy statement from the Commercial Connect LLC.

2.0 Scope

This policy covers appropriate use of any email sent from a Commercial Connect LLC email address and applies to all employees, vendors, and agents operating on behalf of Commercial Connect LLC.

3.0 Policy

3.1 Prohibited Use.

The Commercial Connect LLC email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Commercial Connect LLC employee should report the matter to their supervisor immediately.

3.2 Personal Use.

Using a reasonable amount of Commercial Connect LLC resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Commercial Connect LLC email account is prohibited. Virus or other malware warnings and mass mailings from Commercial Connect LLC shall be approved by Commercial Connect LLC VP Operations before sending. These restrictions also apply to the forwarding of mail received by a Commercial Connect LLC employee.

3.3 Monitoring

Commercial Connect LLC employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system. Commercial Connect LLC may monitor messages without prior notice. Commercial Connect LLC is not obliged to monitor email messages.

4.0 Enforcement

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

5.0 Definitions

Term	**Definition**
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to Commercial Connect LLC or its customers' reputation or market standing.
Virus warning.	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Commercial Connect LLC, who do not have a need to know that information.

6.0 Revision History

Email Retention Policy

Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

Scope

This email retention policy is secondary to Commercial Connect LLC policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All Commercial Connect LLC email information is categorized into four main classifications with retention guidelines:
Administrative Correspondence (4 years)

Fiscal Correspondence (4 years)

General Correspondence (1 year)

Ephemeral Correspondence (Retain until read, destroy)

Policy

3.1 Administrative Correspondence

Commercial Connect LLC Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative

Correspondence is retained, a mailbox admin@Commercial Connect LLC has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.2 Fiscal Correspondence

Commercial Connect LLC Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@Commercial Connect LLC has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.3 General Correspondence

Commercial Connect LLC General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence

Commercial Connect LLC Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Instant Messenger Correspondence

Commercial Connect LLC Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

3.6 Encrypted Communications

Commercial Connect LLC encrypted communications should be stored in a manner consistent with Commercial Connect LLC Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.7 Recovering Deleted Email via Backup Media

Commercial Connect LLC maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

Enforcement

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

Definitions

Terms and Definitions

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Commercial Connect LLC is done via a license. Please contact the appropriate support organization if you require a license.

Approved Instant Messenger

The Jabber Secure IM Client is the only IM that is approved for use on Commercial Connect LLC computers.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Commercial Connect LLC.

Encryption

Secure Commercial Connect LLC Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Revision History

28 July, 2003 Added discussion of backup media

Employee Internet Use Monitoring and Filtering Policy

1.0 Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within Commercial Connect LLC's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

2.0 Scope

This policy applies to all Commercial Connect LLC employees, contractors, vendors and agents with a Commercial Connect LLC-owned or personally-owned computer or workstation connected to the Commercial Connect LLC network.
This policy applies to all end user initiated communications between Commercial Connect LLC’s network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

3.0 Policy

3.1 Web Site Monitoring

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

3.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to the Information Technology Department. Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

3.3 Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Commercial Connect LLC's corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

3.4 Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

3.5 Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

4.0 Enforcement

The IT Security Officer will periodically review Internet use monitoring and filtering systems and processes to ensure they are in compliance with this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Internet Filtering – Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

User ID – User Name or other identifier used when an associate logs into the corporate network.

IP Address – Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

SMTP – Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.

Peer to Peer File Sharing – Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Social Networking Services – Internet sites such as Myspace and Facebook that allow users to post content, chat, and interact in online communities.

SPAM – Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

Hacking – Sites that provide content about breaking or subverting computer security controls.

6.0 Revision History

11/23/2007 – Draft Completed, Kevin Bong

Technology Equipment Disposal Policy

1.0 Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Commercial Connect LLC data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

2.0 Purpose

This policy has been developed to define the requirements for proper disposal of technology equipment at Commercial Connect LLC.

3.0 Scope

This policy applies to all technology equipment owned by Commercial Connect LLC.

4.0 Policy

4.1 Technology Equipment Disposal

1. When technology assets have reached the end of their useful life they should be sent to the local Information Technology office for proper disposal.
2. Information Technology will securely erase all storage mediums in accordance with current industry best practices.
3. Equipment which is working, but reached the end of its useful life to Commercial Connect LLC, will be made available for purchase by employees.
4. A lottery system will be used to determine who has the opportunity to purchase available equipment.
5. All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.
6. Finance and Information Technology will determine an appropriate cost for each item.
7. All purchases are final. No warranty or support will be provided with any equipment sold.
8. Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.

9. Prior to leaving Commercial Connect LLC premises, all equipment must be removed from the Information Technology inventory system.

4.2 Commercial Connect LLC Ramifications

Failure to properly dispose of technology equipment can have several negative ramifications to the Commercial Connect LLC including fines, negative customer perception and costs to notify constituents of data loss or inadvertent disclosure.

5.0 Enforcement

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

6.0 Definitions

Terms	**Definitions**

7.0 Revision History

Ethics Policy

Overview

Commercial Connect LLC purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Commercial Connect LLC employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

Commercial Connect LLC is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Commercial Connect LLC addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Commercial Connect LLC will not tolerate any wrongdoing or impropriety at anytime. Commercial Connect LLC will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Commercial Connect LLC, including all personnel affiliated with third parties.

Policy

Executive Commitment to Ethics

Top brass within Commercial Connect LLC must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

Executives must disclose any conflict of interests regard their position within Commercial Connect LLC.

Employee Commitment to Ethics

Commercial Connect LLC employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

Every employee needs to apply effort and intelligence in maintaining ethics value.

Employees must disclose any conflict of interests regard their position within Commercial Connect LLC.

Employees will help Commercial Connect LLC to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

Company Awareness

Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

Commercial Connect LLC will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

Maintaining Ethical Practices

Commercial Connect LLC will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

Employees at Commercial Connect LLC should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

Commercial Connect LLC has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

Unethical Behavior

Commercial Connect LLC will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

Commercial Connect LLC will not tolerate harassment or discrimination.

Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

Commercial Connect LLC will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

Commercial Connect LLC employees will not use corporate assets or business relationships for personal use or gain.

Enforcement

Any infractions of this code of ethics will not be tolerated and Commercial Connect LLC will act quickly in correcting the issue if the ethical code is broken.

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

Extranet Policy

1.0 Purpose

This document describes the policy under which third party organizations connect to Commercial Connect LLC networks for the purpose of transacting business related to Commercial Connect LLC.

2.0 Scope

Connections between third parties that require access to non-public Commercial Connect LLC resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for Commercial Connect LLC or to the Public Switched Telephone Network does NOT fall under this policy.

3.0 Policy

3.1 Pre-Requisites

3.1.1 Security Review

All new extranet connectivity will go through a security review with the Information Security department (InfoSec). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

3.1.2 Third Party Connection Agreement

All new connection requests between third parties and Commercial Connect LLC require that the third party and Commercial Connect LLC representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Vice President of the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into Commercial Connect LLC labs are to be kept on file with the [name of team responsible for security of labs].

3.1.3 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the [name of team responsible for security of labs]. Typically this function is handled as part of the Third Party Agreement.

3.1.4 Point Of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

3.2 Establishing Connectivity

Sponsoring Organizations within Commercial Connect LLC that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage InfoSec to address security issues inherent in the project. If the proposed connection is to terminate within a lab at Commercial Connect LLC, the Sponsoring Organization must engage the [name of team responsible for security of labs]. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and InfoSec, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Commercial Connect LLC rely upon the third party to protect Commercial Connect LLC's network or resources.

3.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or InfoSec when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within Commercial Connect LLC must notify the extranet team responsible for that connectivity, which will then terminate the access. This may *mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct Commercial Connect LLC business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct Commercial Connect LLC business necessitate a modification of existing permissions, or termination of connectivity, InfoSec and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.*

4.0 Enforcement

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

5.0 Definitions

Terms	*Definitions*
Circuit	*For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.*
Sponsoring Organization	*The Commercial Connect LLC organization who requested that the third party have access into Commercial Connect LLC.*
Third Party	*A business that is not a formal or subsidiary part of Commercial Connect LLC.*

6.0 Revision History

Information Sensitivity Policy

Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Commercial Connect LLC without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Commercial Connect LLC Confidential information (e.g., Commercial Connect LLC Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

Scope

All Commercial Connect LLC information is categorized into two main classifications:

- *Commercial Connect LLC Public*
- *Commercial Connect LLC Confidential*

Commercial Connect LLC Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Commercial Connect LLC Systems, Inc.

Commercial Connect LLC Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Commercial Connect LLC Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Commercial Connect LLC Confidential information is "Commercial Connect LLC Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Commercial Connect LLC by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Commercial Connect LLC's network to support our operations.

Commercial Connect LLC personnel are encouraged to use common sense judgment in securing Commercial Connect LLC Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Commercial Connect LLC Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Commercial Connect LLC Confidential information in question.

Minimal Sensitivity: *General corporate information; some personnel and technical information*

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Commercial Connect LLC Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Commercial Connect LLC Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Commercial Connect LLC information is presumed to be "Commercial Connect LLC Confidential" unless expressly determined to be Commercial Connect LLC Public information by a Commercial Connect LLC employee with authority to do so.

Access: *Commercial Connect LLC employees, contractors, people with a business need to know.*

Distribution within Commercial Connect LLC: *Standard interoffice mail, approved electronic mail and electronic file transmission methods.*

Distribution outside of Commercial Connect LLC internal mail*: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.*

Electronic distribution: *No restrictions except that it be sent to only approved recipients.*

Storage: *Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.*

Disposal/Destruction: *Deposit outdated paper information in specially marked disposal bins on Commercial Connect LLC premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.*

Penalty for deliberate or inadvertent disclosure: *Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.*

More Sensitive: *Business, financial, technical, and most personnel information*

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Commercial Connect LLC Confidential" or "Commercial Connect LLC Proprietary", wish to label the information "Commercial Connect LLC Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access*:* *Commercial Connect LLC employees and non-employees with signed non-disclosure agreements who have a business need to know.*

Distribution within Commercial Connect LLC: *Standard interoffice mail, approved electronic mail and electronic file transmission methods.*

Distribution outside of Commercial Connect LLC internal mail*:* *Sent via U.S. mail or approved private carriers.*

Electronic distribution: *No restrictions to approved recipients within Commercial Connect LLC, but should be encrypted or sent via a private link to approved recipients outside of Commercial Connect LLC premises.*

Storage: *Individual access controls are highly recommended for electronic information.*

Disposal/Destruction: *In specially marked disposal bins on Commercial Connect LLC premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.*

Penalty for deliberate or inadvertent disclosure: *Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.*

Most Sensitive: *Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company*

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Commercial Connect LLC Confidential information is very sensitive, you may should label the information "Commercial Connect LLC Internal: Registered and Restricted", "Commercial Connect LLC Eyes Only", "Commercial Connect LLC Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Commercial Connect LLC Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: *Only those individuals (Commercial Connect LLC employees and non-employees) designated with approved access and signed non-disclosure agreements.*

Distribution within Commercial Connect LLC: *Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.*

Distribution outside of Commercial Connect LLC internal mail: *Delivered direct; signature required; approved private carriers.*

Electronic distribution: *No restrictions to approved recipients within Commercial Connect LLC, but it is highly recommended that all information be strongly encrypted.*

Storage: *Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.*

Disposal/Destruction: *Strongly Encouraged: In specially marked disposal bins on Commercial Connect LLC premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.*

Penalty for deliberate or inadvertent disclosure: *Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.*

Enforcement

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

Terms and Definitions

Appropriate measures

To minimize risk to Commercial Connect LLC from an outside business connection. Commercial Connect LLC computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Commercial Connect LLC corporate information, the amount of information at risk is minimized.

Configuration of Commercial Connect LLC-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Commercial Connect LLC is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources

Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use man chmod to find out more about it). On Mac’s and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Commercial Connect LLC.

Encryption

Secure Commercial Connect LLC Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to Commercial Connect LLC's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that Commercial Connect LLC has control over it's entire distance. For example, all Commercial Connect LLC networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Commercial Connect LLC also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Commercial Connect LLC has established private links include all announced acquisitions and some short-term temporary links

Revision History

Internet usage Policy

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

Consequences of Violations

Violations of the Internet usage Policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the Internet via company network is approved, the potential Internet user is required to read this Internet usage Policy and sign an acknowledgment form (located on the last page of this document). The signed acknowledgment form should be turned in and will be kept on file at the facility granting the access. For questions on the Internet usage Policy, contact the Information Technology (IT) Department.

USAGE THREATS

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

2.1 Inappropriate Use of Resources

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

2.2 Misleading or False Information

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

INTERNET SERVICES

Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

3.1 User Services

3.1.1 Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).

Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.

File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.

Telnet -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.

Management reserves the right to add or delete services as business needs change or conditions warrant. All other services will be considered unauthorized access to/from the Internet and will not be allowed.

3.2 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

3.2.1 Request for Internet Access

As part of the Internet access request process, the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

3.2.2 Approval

Internet access is requested by the user or user’s manager submitting an IT Access Request form to the IT department along with an attached copy of a signed Internet usage Coverage Acknowledgment Form.

3.2.3 Removal of privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

4. USAGE POLICIES

4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

- *Communication between employees and non-employees for business purposes;*
- *IT technical support downloading software upgrades and patches;*
- *Review of possible vendor web sites for product information;*
- *Reference regulatory or technical information.*
- *Research*

4.3 Personal Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

4.4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- *Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.*
- *Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.*
- *Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.*
- *Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.*
- *Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.*
- *Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.*
- *Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.*
- *Any form of gambling.*

  Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:
- *Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.*
- *Any ordering (shopping) of items or services on the Internet.*
- *Playing of any games.*

- *Forwarding of chain letters.*
- *Participation in any on-line contest or promotion.*
- *Acceptance of promotional gifts.*

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

If you have any questions about Acceptable Use, contact the IT Department

4.5 Software License

The company strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as i

4.6 Review of Public Information

All publicly-writeable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with company business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.

4.7 Expectation of Privacy

4.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

4.7.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

4.8 Maintaining Corporate Image

4.8.1 Representation

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

4.8.2 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee's manager and the public relations department and will be placed by an authorized individual.

4.8.3 Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through the IT Department. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the Corporate Communications Directors for initial approval to continue. All company pages are owned by, and are the ultimate responsibility of, the Corporate Communications Directors.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

4.9 Periodic Reviews

4.9.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

4.9.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

5. REFERENCES

5.1 Points of Contact

If you need assistance regarding the following topics related to Internet usage, contact the IT Department for additional assistance:

Corporate Level:
Acceptable Use Public Representation Web Site Legal Department Corporate Communications Directors Corporate Principles
Regional Level:
Access or Connection Problems

6. INTERNET USAGE COVERAGE ACKNOWLEDGMENT FORM

After reading this policy, please sign the coverage form and submit it to your facility's IT department or granting facility's IT department for filing.

By signing below, the individual requesting Internet access through company computing resources hereby acknowledges receipt of and compliance with the Internet Usage Policy. Furthermore, the undersigned also acknowledges that he/she has read and understands this policy before signing this form.

Internet access will not be granted until this acknowledgment form is signed by the individual's manager. After completion, the form is filed in the individual's human resources file (for permanent employees), or in a folder specifically dedicated to Internet access (for contract workers, etc.), and maintained by the IT department. These acknowledgment forms are subject to internal audit.

ACKNOWLEDGMENT

I have read the Internet Usage Policy. I understand the contents, and I agree to comply with the said Policy.

Location (Location and address)

Business Purpose

Name

Signature _________________________________Date ___________________

Manager/Supervisor Signature__________________Date ____________

Mobile Employee Endpoint Responsibility Policy

1.0 Purpose

This document describes Information Security's requirements for employees of Commercial Connect LLC that work outside of an office setting.

2.0 Scope

This policy applies to any mobile device, or endpoint computer issued by Commercial Connect LLC or used for Commercial Connect LLC business which contains stored data owned by Commercial Connect LLC.

3.0 Policy

All employees shall assist in protecting devices issued by Commercial Connect LLC or storing Commercial Connect LLC data. Mobile devices are defined to include desktop systems in a telework environment, laptops, PDAs, and cell phones.

Users are expressly forbidden from storing Commercial Connect LLC data on devices that are not issued by Commercial Connect LLC, such as storing Commercial Connect LLC email on a personal cell phone or PDA.

3.1 Anti-Virus, Secunia CSI and Endpoint Security Software

Commercial Connect LLC will issue computers with Secunia, Anti-virus and Endpoint security installed. Employees are to notify the security department immediately if they see error messages for these products. Employees shall run on online malware scanner at least once a month for a "second opinion", see Commercial Connect LLC Microsoft Security and Privacy Manual for approved scanners.

3.2 Browser Addons

In general, Commercial Connect LLC does not recommend using Browser Addons, however we do not forbid the use of these tools if they enhance productivity. After installing a Browser Addon, employees shall run a browser testing tool. See Commercial Connect LLC Microsoft Security and Privacy Manual for testing tools.

4.0 Enforcement

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

5.0 Revision History

1.0 initial policy version, 10/29/2008

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Commercial Connect LLC's resources. All users, including contractors and vendors with access to Commercial Connect LLC systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Commercial Connect LLC facility, has access to the Commercial Connect LLC network, or stores any non-public Commercial Connect LLC information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

All users at Commercial Connect LLC should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least fifteen alphanumeric characters.

Weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Commercial Connect LLC", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

(NOTE: Do not use either of these examples as passwords!)

B. Password Protection Standards

- Always use different passwords for Commercial Connect LLC accounts from other non-Commercial Connect LLC access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various Commercial Connect LLC access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share Commercial Connect LLC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Commercial Connect LLC information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

If an account or password compromise is suspected, report the incident to the Information Security Department.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the Commercial Connect LLC Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Department or its delegates. If a password is guessed or cracked during these excersises, the user/owner will be required to change it.

6.0 Terms and Definitions

Term	Definition
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Personal Communication Devices and Voicemail Policy

1.0 Purpose

This document describes Information Security's requirements for Personal Communication Devices and Voicemail for Commercial Connect LLC.

2.0 Scope

This policy applies to any use of Personal Communication Devices and Commercial Connect LLC Voicemail issued by Commercial Connect LLC or used for Commercial Connect LLC business.

3.0 Policy

3.1 Issuing Policy

Personal Communication Devices (PCDs) will be issued only to Commercial Connect LLC personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, to Commercial Connect LLC personnel who need to conduct immediate, critical <Company> business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

3.2 Bluetooth

Hands-free enabling devices, such as the Bluetooth, may be issued to authorized Commercial Connect LLC personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters, Bluetooth 2.0 Class 1 devices have a range of 330 feet.

3.3 Voicemail

Voicemail boxes may be issued to Commercial Connect LLC personnel who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.

3.4 Loss and Theft

Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

3.5 Personal Use

PCDs and voicemail are issued for Commercial Connect LLC business. Personal use should be limited to minimal and incidental use.

3.6 PCD Safety

Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If employees must use a PCD while driving, Commercial Connect LLC requires the use of hands-free enabling devices.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action that leads to being ineligible for continued use of PCDs. Extreme cases could lead to additional discipline, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Bluetooth	Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), and mobile phones via a secure, globally unlicensed short-range radio frequency. Source: Wikipedia
Confidential or sensitive data	All data that is not approved for public release shall be considered confidential or sensitive.

6.0 Revision History

Remote Access Policy

1.0 Purpose

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

2.0 Scope

This policy applies to all Commercial Connect LLC employees, contractors, vendors and agents with a Commercial Connect LLC-owned or personally-owned computer or workstation used to connect to the Commercial Connect LLC network. This policy applies to remote access connections used to do work on behalf of
Commercial Connect LLC, 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, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of Commercial Connect LLC employees, contractors, vendors and agents with remote access privileges to Commercial Connect LLC's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Commercial Connect LLC.
2. General access to the Internet for recreational use by immediate household members through the Commercial Connect LLC Network on personal computers is permitted for employees that have flat-rate services. The Commercial Connect LLC employee is responsible to ensure the family member does not violate any Commercial Connect LLC policies, does not perform illegal activities, and does not use the access for outside business interests. The Commercial Connect LLC employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Commercial Connect LLC's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding Commercial Connect LLC's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

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.
2. At no time should any Commercial Connect LLC employee provide their login or email password to anyone, not even family members.
3. Commercial Connect LLC employees and contractors with remote access privileges must ensure that their Commercial Connect LLC-owned or personal computer or workstation, which is remotely connected to Commercial Connect LLC'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. Commercial Connect LLC employees and contractors with remote access privileges to Commercial Connect LLC's corporate network must not use non-Commercial Connect LLC email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Commercial Connect LLC business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Commercial Connect LLC network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to Commercial Connect LLC 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*.
10. Personal equipment that is used to connect to Commercial Connect LLC's networks must meet the requirements of Commercial Connect LLC-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Commercial Connect LLC production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

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

5.0 Definitions

Term	**Definition**
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem

A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing

Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Commercial Connect LLC-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Commercial Connect LLC and an ISP, depending on packet destination.

DSL

Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay

A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN

There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access

Any access to Commercial Connect LLC's corporate network through a non-Commercial Connect LLC controlled network, device, or medium.

Split-tunneling

Simultaneous direct access to a non-Commercial Connect LLC network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Commercial Connect LLC's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Removable Media

1.0 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

2.0 Purpose

To minimize the risk of loss or exposure of sensitive information maintained by Commercial Connect LLC and to reduce the risk of acquiring malware infections on computers operated by Commercial Connect LLC.

3.0 Scope

This policy covers all computers and servers operating in Commercial Connect LLC.

4.0 Policy

Commercial Connect LLC staff may only use Commercial Connect LLC removable media in their work computers. Commercial Connect LLC removable media may not be connected to or used in computers that are not owned or leased by the Commercial Connect LLC without explicit permission of the Commercial Connect LLC info sec staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Commercial Connect LLC Acceptable Encryption Policy:

Exceptions to this policy may be requested on a case-by-case basis by Commercial Connect LLC-exception procedures.

5.0 Enforcement

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

6.0 Definitions

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by Commercial Connect LLC.

Encryption: A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Sensitive Information: Information which, if made available to unauthorized persons, may adversely affect Commercial Connect LLC, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers and, financial information,

Malware: Software of malicious intent/impact such as viruses, worms, and Spyware.

7.0 Revision History

Original Issue Date:

Risk Assessment Policy

1.0 Purpose

To empower InfoSec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope

Risk assessments can be conducted on any entity within Commercial Connect LLC or any outside entity that has signed a *Third Party Agreement* with Commercial Connect LLC. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs is the joint responsibility of InfoSec and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the InfoSec Risk Assessment Team in the development of a remediation plan.

4.0 Risk Assessment Process

For additional information, go to the Risk Assessment Process.

5.0 Enforcement

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

6.0 Definitions

Terms **Definitions**

Entity Any business unit, department, group, or third party, internal or external to Commercial Connect LLC, responsible for maintaining Commercial Connect LLC assets.

Risk Those factors that could affect confidentiality, availability, and integrity of Commercial Connect LLC's key information assets and systems. InfoSec is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History

Router Security Policy

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Commercial Connect LLC.

2.0 Scope

All routers and switches connected to Commercial Connect LLC production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
   a. IP directed broadcasts
   b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
   c. TCP small services
   d. UDP small services
   e. All source routing
   f. All web services running on router
4. Use corporate standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the corporate enterprise management system with a designated point of contact.
7. Each router must have the following statement posted in clear view:

   "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

8. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

4.0 Enforcement

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

5.0 Definitions

Terms	**Definitions**
Production Network	The "production network" is the network used in the daily business of Commercial Connect LLC. Any network connected to the corporate backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to Commercial Connect LLC employees or impact their ability to do work.
Lab Network	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to Commercial Connect LLC nor affect the production network.

6.0 Revision History

2007-04-18

- *Added 3.0.8 “Telnet”*

Server Audit Policy

1.0 Purpose

The purpose of this policy is to ensure all servers deployed at Commercial Connect LLC are configured according to the Commercial Connect LLC security policies. Servers deployed at Commercial Connect LLC shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

- *Ensure integrity, confidentiality and availability of information and resources*
- *Ensure conformance to Commercial Connect LLC security policies*

2.0 Scope

This policy covers all servers owned or operated by Commercial Connect LLC. This policy also covers any server present on Commercial Connect LLC premises, but which may not be owned or operated by Commercial Connect LLC.

3.0 Policy

Commercial Connect LLC hereby provides its consent to allow CAS-Com Internet Services, Inc. to access its servers to the extent necessary to allow <Audit organization> to perform scheduled and ad hoc audits of all servers at Commercial Connect LLC.

3.1 Specific Concerns

Servers in use for Commercial Connect LLC support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of these systems.

3.2 Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include:

- *All system logs shall be sent to a central log review system*
- *All Sudo / Administrator actions must be logged*
- *Use a central patch deployment system*

- *Host security agent such as antivirus shall be installed and updated*
- *Network scan to verify only required network ports and network shares are in use*
- *Verify administrative group membership*
- *Conduct baselines when systems are deployed and upon significant system changes*
- *Changes to configuration template shall be coordinated with approval of change control board*

3.2 Responsibility

CAS-Com Internet Services, Inc. shall conduct audits of all servers owned or operated by Commercial Connect LLC. Server and application owners are encouraged to also perform this work as needed.

3.4 Relevant Findings

All relevant findings discovered as a result of the audit shall be listed in the Commercial Connect LLC tracking system to ensure prompt resolution or appropriate mitigating controls.

3.4 Ownership of Audit Report.

All results and findings generated by the CAS-Com Internet Services, Inc. Team must be provided to appropriate Commercial Connect LLC management within one week of project completion. This report will become the property of Commercial Connect LLC and be considered company confidential.

4.0 Enforcement

CAS-Com Internet Services, Inc. shall never use access required to perform server audits for any other purpose. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

SERVER MALWARE PROTECTION POLICY

1.0 Overview:

Commercial Connect LLC is entrusted with the responsibility to provide professional management of clients servers as outlined in each of the contracts with its customers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

2.0 Purpose:

The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

3.0 Scope:

This policy applies to all servers that Commercial Connect LLC is responsible to manage. This explicitly includes any system for which Commercial Connect LLC has a contractual obligation to administer. This also includes all server systems setup for internal use by Commercial Connect LLC, regardless of whether Commercial Connect LLC retains administrative obligation or not.

4.0 Policy:

Commercial Connect LLC operations staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

4.1 ANTI-VIRUS

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- *Non-administrative users have remote access capability*
- *The system is a file server*
- *NBT/Microsoft Share access is open to this server from systems used by non-administrative users*
- *HTTP/FTP access is open from the Internet*

Other "risky" protocols/applications are available to this system from the Internet at the discretion of the Commercial Connect LLC Security Administrator

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- *Outbound web access is available from the system*

4.2 MAIL SERVER ANTI-VIRUS

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

4.3 ANTI-SPYWARE

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- *Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet*
- *Any system where non-technical or non-administrative users have the ability to install software on their own*

4.4 NOTABLE EXCEPTIONS

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions apply to this system:

- *The system is a SQL server*
- *The system is used as a dedicated mail server*
- *The system is not a Windows based platform*

5.0 Enforcement:

The responsibility for implementing this policy belongs to all operational staff at Commercial Connect LLC. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the Commercial Connect LLC Security Officer. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions:

TERM *DEFINITION*

Server *For purposes of this policy, a server is any computer system residing in the physically secured data center owned and operated by Commercial Connect LLC. In addition, this includes any system running an operating system specifically intended for server usage as defined by the Commercial Connect LLC IT/IS Manager that has access to internal secure networks. This includes, but is not limited to, Microsoft Server 2000 and all permutations, Microsoft Server 2003 and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to and VMS.*

Malware *Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.*

Spyware *Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.*

Anti-virus Software *Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).*

7.0 Revision History:

8.0 References:

“Malware.” Wikipedia, The Free Encyclopedia. 08 Nov 2006,

< http://en.wikipedia.org/wiki/Malware>

"Spyware." Wikipedia, The Free Encyclopedia. 08 Nov 2006,

<http://en.wikipedia.org/wiki/Spyware>

"Anti-Virus." Wikipedia, The Free Encyclopedia. 08 Nov 2006

< http://en.wikipedia.org/wiki/Anti-virus>

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Commercial Connect LLC. Effective implementation of this policy will minimize unauthorized access to Commercial Connect LLC proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by Commercial Connect LLC, and to servers registered under any Commercial Connect LLC-owned internal network domain.

This policy is specifically for equipment on the internal Commercial Connect LLC network. For secure configuration of equipment external to Commercial Connect LLC on the DMZ, refer to the Internet DMZ Equipment Policy.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at Commercial Connect LLC must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.

- *Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:*
    - *Server contact(s) and location, and a backup contact*
    - *Hardware and Operating System/Version*
    - *Main functions and applications, if applicable*
- *Information in the corporate enterprise management system must be kept up-to-date.*
- *Configuration changes for production servers must follow the appropriate change management procedures.*

3.2 General Configuration Guidelines

- *Operating System configuration should be in accordance with approved InfoSec guidelines.*
- *Services and applications that will not be used must be disabled where practical.*
- *Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.*
- *The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.*
- *Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.*
- *Always use standard security principles of least required access to perform a function.*
- *Do not use root when a non-privileged account will do.*
- *If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).*
- *Servers should be physically located in an access-controlled environment.*
- *Servers are specifically prohibited from operating from uncontrolled cubicle areas.*

3.3 Monitoring

- *All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:*
    - *All security related logs will be kept online for a minimum of 1 week.*
    - *Daily incremental tape backups will be retained for at least 1 month.*
    - *Weekly full tape backups of logs will be retained for at least 1 month.*
    - *Monthly full backups will be retained for a minimum of 2 years.*
- *Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:*
    - *Port-scan attacks*
    - *Evidence of unauthorized access to privileged accounts*
    - *Anomalous occurrences that are not related to specific applications on the host.*

3.4 Compliance

- *Audits will be performed on a regular basis by authorized organizations within Commercial Connect LLC.*
- *Audits will be managed by the internal audit group or InfoSec, in accordance with the Audit Policy. InfoSec will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.*
- *Every effort will be made to prevent audits from causing operational failures or disruptions.*

4.0 Enforcement

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

5.0 Definitions

Term	***Definition***
DMZ	*De-militariezed Zone. A network segment external to the corporate production network.*
Server	*For purposes of this policy, a Server is defined as an internal Commercial Connect LLC Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.*

6.0 Revision History

SOCIAL ENGINEERING AWARENESS Employee Front Desk Communication & Awareness Policy

1.0 Overview

The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of Commercial Connect LLC. This Employee Front Desk Communication Policy is part of the Social Engineering Awareness Policy bundle.

In order to protect Commercial Connect LLC's assets, all employees need to defend the integrity and confidentiality of Commercial Connect LLC's resources.

2.0 Purpose

This policy has two purposes:

1. *To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks.*

   Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.

   Employees know who to contact in these circumstances.

   Employees recognize they are an important part of Commercial Connect LLC's security. The integrity of an employee is the best line of defense for protecting sensitive information regarding Commercial Connect LLC's resources.

2. *To create specific procedures for employees to follow to help them make the best choice when:*

   Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect Commercial Connect LLC's sensitive information.

   The employee is being "socially pressured" or "socially encouraged or tricked" into sharing sensitive data.

3.0 Scope

Includes all employees of Commercial Connect LLC, including temporary contractors or part-time employees participating with help desk customer service.

4.0 Policy

Sensitive information of Commercial Connect LLC will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

- *An "urgent matter"*
- *A "forgotten password"*
- *A "computer virus emergency"*
- *Any form of intimidation from "higher level management"*
- *Any "name dropping" by the individual which gives the appearance that it is coming from legitimate and authorized personnel.*

The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of Commercial Connect LLC resources.

The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.

The techniques are used by a person that declares to be "affiliated" with Commercial Connect LLC such as a sub-contractor.

The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.

The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

5.0 Action

All persons described in section 3.0 MUST attend the security awareness training within 30 days from the date of employment and every 6 months thereafter.

5.1.1 If one or more circumstances described in section 4.0 is detected by a person described in section 3.0, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.

5.1.2 If the identity of the requester described in section 5.1.1 CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.

5.1.3 If the supervisor or manager is not available, that person MUST contact the security personnel.

5.1.4. If the security personnel is not available, the person described in section 3.0 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

6.0 Enforcement

6.1.0 All persons described in section 3.0 who (a) successfully detect circumstances set forth in section 4.0 and (b) correctly complete an action described in section 5.0 are entitled to have an extra day off at the discretion of their direct supervisor or manager.

6.1.1 All persons described in section 3.0 who violate this policy may be subject to temporary suspension from work and must attend Commercial Connect LLC's security awareness training again before being readmitted.

7.0 Revision History

7.1.0 Policy is in effect starting July 16, 2009; Version 1.0, Emilio Valente

7.1.1 Document revised (date, version and author): ______

THIRD PARTY CONNECTION AGREEMENT

This Third Party Network Connection Agreement (the "Agreement") by and between <Your Company Name>, a <Your Company's State> corporation, with principal offices at <Your Address>, <Your Company's State>, ("<Your Company>") and ________________________ , a _________________ corporation, with principal offices at ________________________________ ("Company"), is entered into as of the date last written below ("the Effective Date").

This Agreement consists of this signature page and the following attachments that are incorporated in this Agreement by this reference:

1. Attachment 1: Third Party Network Connection Agreement Terms and Conditions
2. Attachment 2 Network Connection Policy
3. Attachment 3: Third Party Connection Request - Information Requirements Document
4. Attachment 4: <Your Company> Non-Disclosure Agreement
5. Attachment 5: <Your Company> Equipment Loan Agreement

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by <Your Company's State> law without regard to choice of law provisions.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

___________________ (“Company”)	*<Your Company Name> (“<Your Company>”)*
___________________	_____________________________
Authorized Signature	*Authorized Signature*
___________________	_____________________________
Name	*Name*
___________________	_____________________________
Date	*Date*

Attachment 1

THIRD PARTY CONNECTION AGREEMENT

TERMS AND CONDITIONS

Object: *To ensure that a secure method of connectivity is provided between <Your Company> and Company and to provide guidelines for the use of network and computing resources associated with the Network Connection as defined below.*

Definition: *"Network Connection" means one of the <Your Company> connectivity options listed in Section B of the Network Connection Policy.*

1. *Right to Use Network Connection. Company may only use the Network Connection for business purposes as outlined by the* ***Third Party Connection Request - Information Requirements Document****.*

2. *<Your Company>-Owned Equipment.*

2.1 *<Your Company> may, in <Your Company> sole discretion, loan to Company certain equipment and/or software for use on Company premises (the <Your Company>-Owned Equipment) under the terms of the <Your Company> Equipment Loan Agreement set forth in Attachment 5. <Your Company>-Owned Equipment will only be configured for TCP/IP, and will be used solely by Company on Company's premises and for the purposes set forth in this Agreement.*

2.2 *Company may modify the configuration of the <Your Company>-Owned Equipment only after notification and approval in writing by authorized <Your Company> personnel.*

2.3 *Company will not change or delete any passwords set on <Your Company>-Owned Equipment without prior approval by authorized <Your Company> personnel. Promptly upon any such change, Company shall provide <Your Company> with such changed password.*

3. Network Security.

3.1 Company will allow only Company employees approved in advance by <Your Company> ("Authorized Company Employees") to access the Network Connection or any <Your Company>-Owned Equipment. Company shall be solely responsible for ensuring that Authorized Company Employees are not security risks, and upon <Your Company>'s request, Company will provide <Your Company> with any information reasonably necessary for <Your Company> to evaluate security issues relating to any Authorized Company Employee. Access to the Network Connection or any <Your Company>-Owned Equipment

3.2 Company will promptly notify <Your Company> whenever any Authorized Company Employee leaves Company's employ or no longer requires access to the Network Connection or <Your Company>-Owned Equipment.

3.3 Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the Network Connection (and Company's use of <Your Company>-Owned Equipment) is secure and is used only for authorized purposes, and (b) such party's business records and data are protected against improper access, use, loss alteration or destruction.

4. Notifications. Company shall notify <Your Company> in writing promptly upon a change in the user base for the work performed over the Network Connection or whenever in Company's opinion a change in the connection and/or functional requirements of the Network Connection is necessary.

5. Payment of Costs. Each party will be responsible for all costs incurred by that party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

6. DISCLAIMER OF WARRANTIES. NEITHER PARTY MAKES ANY WARRANTIES, EXPRESSED OR IMPLIED, CONCERNING ANY SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY. EXCEPT WITH RESPECT TO A PARTY'S CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM ANY DELAY, OMISSION OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF DATA PURSUANT TO THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON

CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, AND WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

8. Confidentiality. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the others technology and products that is confidential and of substantial value to that party, which value would be impaired if such information were disclosed to third parties ("Confidential Information"). Should such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure. Each party agrees that it will not use in any way for its own account, except as provided herein, nor disclose to any third party, any such Confidential Information revealed to it by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information. Upon request by the receiving party, the disclosing party shall advise whether or not it considers any particular information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information. The receiving party's obligation of confidentiality shall not apply to information that: (a) is already known to the receiving party or is publicly available at the time of disclosure; (b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or (c) becomes publicly available after disclosure through no fault of the receiving party.

9. Term, Termination and Survival. This Agreement will remain in effect until terminated by either party. Either party may terminate this agreement for convenience by providing not less than thirty (30) days prior written notice, which notice will specify the effective date of termination. Either party may also terminate this Agreement immediately upon the other party's breach of this Agreement. Sections 5, 6, 7, 8, 10.1 and 10.2 shall survive any termination of this Agreement.

10. MISCELLANEOUS.

10.1 Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

10.2 Waiver. The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

10.3 <u>Assignment</u>. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.

10.4 <u>Force Majeure</u>. Neither party will be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

Attachment2

NETWORK CONNECTION POLICY

Purpose: *To ensure that a secure method of network connectivity between <Your Company> and all third parties and to provide a formalized method for the request, approval and tracking of such connections.*

Scope: *External company data network connections to <Your Company> can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the <Your Company> network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts. Therefore, all external company data network connections will be via the Global Partners Network. This policy applies to all new Third Party Network Connection requests and any existing Third Party Network Connections. When existing Third Party Network Connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed*

Definitions: *A "Network Connection" is defined as one of the connectivity options listed in Section B. below. "Third Parties" is defined as <Your Company> Partners, Vendors, Suppliers and the like.*

A. Third-Party Connection Requests and Approvals

All requests for Third Party connections must be made using the appropriate method based on the support organization. [Add text about the specific support methods]

The required information is outlined in the ***Third Party Connection Request - Information Requirements Document*** *(See Attachment 3 of this document). All information requested on this form must be completed prior to approval and sign off. It is Company's responsibility to ensure that Company has provided all of the necessary information and that such information is correct.*

All Third Party connection requests must have a <Your Company> VP level signature for approval. In some cases approval may be given at a lower level with pre-authorization from the appropriate <Your Company> VP. Also, all Third Parties requesting a Network Connection must complete and sign a <Your Company> Non-Disclosure Agreement.

As a part of the request and approval process, the technical and administrative contact within Company's organization or someone at a higher level within Company will be required to read and sign the "Third Party Connection Agreement " and any additional documents, such as the <Your Company> Non-Disclosure Agreement.

B. Connectivity Options

The following five connectivity options are the standard methods of providing a Third Party Network Connection. Anything that deviates from these standard methods must have a waiver sign-off at the <Your Company> VP level.

1) Leased line (e.g. T1) - Leased lines for Third Parties

will be terminated on the Partners network.

2) ISDN/FR - Dial leased lines will terminate on a Third Party only

router located on the ECS or IT Partners network. Authentication for these

connections must be as stated in Section E. below.

3) Encrypted Tunnel - Encrypted tunnels should[must?] be terminated on

the Partners Network whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel on the dirty subnet, in which case the normal <Your Company> perimeter security measures will control access to Internal devices.

4) Telnet access from Internet - Telnet access from the Internet

will be provided by first telneting to the Third Party gateway machine,

where the connection will be authenticated per Section E. below.

Once the connection is authenticated, telnet sessions to internal

hosts will be limited to those services needed by using the

authorization capabilities of <Your Company>Secure.

5) Remote Dial-up via PPP/SLIP - Remote dial-up via PPP/SLIP will be provided by a separate Third Party modem pool. The connection will be authenticated per Section E. below

C. Third Party (Partner) Access Points

When possible, Third Party (Partner) Access Points (PAPs should be established in locations such that the cost of the access is minimized. Each PAP should consist of at least one router with leased line with Frame Relay and/or ISDN capability.

D. Services Provided

In general, services provided over Third Party Network Connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. ***Blanket access will not be provided for anyone.*** *The default policy position is to deny all access and then only allow those specific services that are needed and approved by <Your Company> pursuant to the established procedure.*

In no case shall a Third Party Network Connection to <Your Company> be used as the Internet connection for the Third Party.

The standard set of allowable services are listed below:

File Exchange via ftp – Where possible, file exchange via ftp should take place on the existing <Your Company> ftp servers (ftp-eng.<Your Company>.com for engineering-related work or ftp.<Your Company>.com for all other work). IT supported Third Party connections have additional FTP services provided by a server in on the Partners Network.

Electronic Mail Exchange – Business-related email exchange between <Your Company> and Third Parties may be conducted over the Network Connection as needed. Mail from Third Party sites to non-<Your Company> addresses will not be allowed over the Network Connection.

Telnet Access – Telnet access will be provided to specific <Your Company> hosts, as needed. Employees from Third Parties will only be given accounts on the specific <Your Company> hosts that are needed. Where possible, router ACLs and static routes will be used to limit the paths of access to other internal <Your Company> hosts and devices. NOTE: NIS accounts and Directory Services are not to be established for employees of Third Parties who have accounts on <Your Company> hosts.

Web Resource Access – Access to internal web resources will be provided on an as-needed basis. Access will be provided by mirroring the appropriate web resources to a web server that resides on the Partners Network. Access to <Your Company>'s public web resources will be accomplished via the normal Internet access for the Third Party.

Access to Source Code Repositories This access will be decided on case by case basis.

Print Services – Print services can be provided to <Your Company> IT-supported Third Party connections by via two print spoolers on the <Your Company> Partners Network. <Your Company>-owned printers, that boot off the print spoolers will be located on the <Your Company> –extended network at the Third Party sites.

SQL*Net Access – This will be decided on a case by case basis.

ERP Access – This will be decided on a case by case basis.

NT File Exchange – File exchange will be provided by NT file servers located on the <Your Company> Partners Network. Each Third Party needing NT File exchange will be provided with a separate folder that is only accessible to that Party and the necessary people at <Your Company>.

E. Authentication for Third Party Network Connections

Third Party Network Connections made via remote dial-up using PPP/SLIP or standard telnet over the Internet will be authenticated using the Partners Authentication database and Token Access System. Currently, <Generic> is the token access system in use. A separate server will be established specifically for Third Parties. Reports showing who

has access via the tokens will be generated monthly and sent to the <Your Company> POCs for each Third Party for verification and review.

Telnet connection made via the Internet must be initiated to a separate which authenticates to the Partners Authentication database and Token Access System mentioned above..

ISDN/FR connections will be authenticated via the Partners <Your Company>Secure database, which is separate from the <Your Company> ISDN authentication database.

F. <Your Company> Equipment at Third Party Sites

In many cases it may be necessary to have <Your Company>-owned and maintained equipment at a Third Party site. All such equipment will be documented on the Third Party Connection Request – Information Requirements Document. Access to network devices such as routers and switches will only be provided to <Your Company> support personnel. All <Your Company>-Owned Equipment located at Third Party sites must be used only for business purposes. Any misuse of access or tampering with <Your Company>-provided hardware or software, except as authorized in writing by <Your Company>, may, in <Your Company>'s sole discretion, result in termination of the connection agreement with the Third Party. If <Your Company> equipment is loaned to a Third Party, the Third Party will be required to sign an appropriate <Your Company> Equipment Loan Agreement, if one is required

G. Protection of Company Private Information and Resources

The <Your Company> network support group responsible for the installation and configuration of a specific Third Party Connection must ensure that all possible measures have been taken to protect the integrity *and privacy of <Your Company> confidential information. At no time should <Your Company> rely on access/authorization control mechanisms at the Third Party's site to protect or prohibit access to <Your Company> confidential information.*

Security of Third Party Connections will be achieved by implementing "Access Control Lists" on the Partner Gateway routers to which the Third Party sites are connected. The ACLs will restrict access to pre-defined hosts within the internal <Your Company> network. The ACLs will be determined by the appropriate support organization. A set of default ACLs may be established as a baseline.

Enable-level access to <Your Company>-owned/maintained routers on Third Party premise will only be provided to the appropriate support organization. All other business personnel (i.e. Partner Site local technical support personnel) will have restricted access/read-only access to the routers at their site and will not be allowed to make configuration changes.

<Your Company> shall not have any responsibility for ensuring the protection of Third Party information. The Third Party shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

H. Audit and Review of Third Party Network Connections

All aspects of Third Party Network Connections - up to, but not including Company's firewall, will be monitored by the appropriate <Your Company> network support group. Where possible, automated tools will be used to accomplish the auditing tasks. Monthly reports should be generated on the Partners Authentication database showing the specific login entries and the appropriate <Your Company> POC. Each <Your Company> Partner POC will receive a copy of the monthly reports showing all of the accounts pertaining to his/her area. Copies of the reports will also be mailed to the department directors.

Nightly audits will be performed on all <Your Company>-owned/maintained Third Party router/network device configurations and the output will be mailed to the appropriate <Your Company> network support group. Any unauthorized changes will be investigated immediately.

All Third Party Network Connections will be reviewed on a quarterly basis and information regarding specific Third Party Network Connection will be updated as necessary. Obsolete Third Party Network Connections will be terminated.

I. <Your Company> Corporate IT Information Security Organization

<Your Company> Corporate IT Information Security has the responsibility for maintaining related policies and standards. Corporate IT Information Security will also provide advice and assistance regarding judgment calls, and will facilitate information gathering in order to make a correct decision. Global coordination of confidentiality and non-disclosure agreements with all third parties is also the responsibility of <Your Company> Corporate IT Information Security.

J. <Your Company> Enterprise Network Services

The Enterprise Network Services Partners Group is responsible for all global firewall design, configuration and engineering required for support of the Global Partners Network.

Attachment 3

THIRD PARTY CONNECTION REQUEST - INFORMATION REQUIREMENTS DOCUMENT

In accordance with the Network Connection Policy, all requests for Third Party Network Connections must be accompanied by this completed Information Requirements Document. This document should be completed by the <Your Company> person or group requesting the Network Connection.

A. Contact Information

Requester Information

Name:

Department Number:

Manager's Name:

Director's Name:

Phone Number:

Email Address:

Technical Contact Information

Name:

Department:

Manager's Name:

Director's Name:

Phone Number:

Pager Number:

Email Address

Back-up Point of Contact:

Name:

Department:

Manager's Name:

Director's Name:

Phone Number:

Pager Number:

Email Address

B. Problem Statement/Purpose of Connection

What is the desired end result? Company must include a statement about the business needs of the proposed connection.

C. Scope of Needs ***(****In some cases, the scope of needs may be jointly determined by the supporting organization and the Third Party.)*

What services are needed? (See Section D. of Network Connection Policy)

What are the privacy requirements (i.e. do you need encryption)?

What are the bandwidth needs?

How long is the connection needed?

Future requirements, if any.

D. Third Party Information

Third Party Name

Management contact (Name, Phone number, Email address)

Location (address) of termination point of the Network Connection (including building number, floor and room number)

Main phone number

Local Technical Support Hours (7X24, etc).

Escalation List

Host/domain names of the Third Party

Names (Email addresses, phone numbers) of all employees of the Third Party who will use this access. If not appropriate to list the names of all employees, then provide a count of the number of employees who will be using the connection.

E. What type of work will be done over the Network Connection?

What applications will be used?

What type of data transfers will be done?

How many files are involved?

What are the estimated hours of use each week? What are peek hours?

F. Are there any known issues such as special services that are required? Are there any unknown issues at this point, such as what internal <Your Company> services are needed?

G. Is a backup connection needed? (e.g., are there any critical business needs associated with this connection?)

H. What is the requested installation date? (Minimum lead-time is 60 days)

I. What is the approximate duration of the Third Party Network Connection?

J. Has a Non-Disclosure Agreement been sign with the Third Party or the appropriate employees of the Third Party?

K. Are there any exiting Network Connections at <Your Company> with this company?

L. Other useful information

Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Commercial Connect LLC corporate network.

2.0 Scope

This policy applies to all Commercial Connect LLC employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Commercial Connect LLC network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy

Approved Commercial Connect LLC employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Commercial Connect LLC internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Commercial Connect LLC network operational groups.
6. All computers connected to Commercial Connect LLC internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from Commercial Connect LLC's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Commercial Connect LLC-owned equipment must configure the equipment to comply with Commercial Connect LLC's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Commercial Connect LLC's network, and as such are subject to the same rules and regulations that apply to Commercial Connect LLC-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.

6.0 Revision History

Visitor and Contractor Premise Access Policy

1.0 Purpose

The purpose of this document is to provide guidance for Visitors to Commercial Connect LLC premises, as well as for employees sponsoring Visitors to Commercial Connect LLC.

2.0 Cancellation or Expiration

The processes and statements in this document do not have an expiry date. However, this document is reviewed and updated annually, and is maintained in the Document Management system of Commercial Connect LLC.

3.0 Background

Commercial Connect LLC is an Engineering and Manufacturing company, delivering quality engineered video products to our customers. As such, we have a significant investment in Intellectual Property. Also, our manufacturing facilities have areas that could be considered hazardous to untrained or unequipped personnel. This document provides the mechanism to protect both our Visitors and the company, while still filling our mandate of community education and participation.

4.0 Scope

This policy applies to all Visitors to any premise of Commercial Connect LLC, and to employees who sponsor Visitors.

5.0 Policy Statement

5.1 Parking

Visitors are encouraged to use designated Visitor Parking spots. If these spots are in use, regular employee parking spots can be used.

5.2 Check-In

All Visitors must arrive at a designated Check-In entrance (the main reception desk in most locations).

All Visitors must present government-issue photo identification at time of Check-In.

All Visitors must be met by their employee sponsor at the time of Check-In.

A Visitor cannot sponsor another Visitor.

Pets are not permitted; however, assistance animals such as Seeing Eye Dogs are permitted. In some cases prior arrangements may be required. Some manufacturing areas (such as assembly clean rooms) are not appropriate for animals under any circumstances.

Visitors must sign two copies of a "Visitor Agreement." Visitors must read this document and keep their copy of this agreement with them at all times during their visit. Visitors will be required to initial the **Emergency Evacuation** *section of this agreement, and will be asked verbally if they have read and understand this section. Visitors will also be required to initial the* **Exit Inspection** *section of this document.*

All Visitor electronics (laptops, other computer equipment, cell phones, etc.) will be checked in as described in the Laptop, Computer and Related Equipment Check-In / Check-Out Procedure.

5.3 Visitor Badges

Visitor Badges must be worn at all time. Employees are instructed to immediately report anyone not wearing a Visitor or Employee badge.

Visitors requiring access to areas controlled by swipe card access locks should arrange temporary cards with their sponsor. Departments that have swipe card access locks in their area may have a small number of temporary swipe cards available. These cards are limited to activation windows of 24 hours.

5.4 Photographs and Cameras

Visitors are not permitted to take photographs inside of Commercial Connect LLC premises, unless discussed specifically with sponsoring employees. For instance, photographs are sometimes required for documentation purposes. If employees have any questions about the suitability of photographs, they should consult the Human Resources Department.

Dedicated cameras are not permitted onsite. Cell phones and laptops equipped with cameras are permitted, but as previously stated photographs are not permitted without permission.

5.5 Information Disclosure

Visitors should not request information that does not pertain to their visit or the work being performed. confidential or otherwise inappropriate nature, requests for corporate documents, customer information, financial projections, comments on any matter currently under litigation, future products or future corporate direction, or requests for information or statements in the name of the company (as might be requested by a reporter or a lawyer) will be reported to the Office of the CSO, and will be dealt with under the "Penalties" section of this document.

5.6 Check-Out

Visitors will check out at the same station where they arrived. All Visitor electronics will be checked out individually as described in the Laptop, Computer and related equipment Check-In /

Check-out Procedure. The checked out Visitor will be taken off the On-Premise List, both in the paper and online copies.

Checking out of computers and related equipment may take significantly longer after regular business hours, Visitors should factor this into their estimates for exit times.

5.7 Exit Inspection

Visitors may be subject to a brief search of their laptop bags or other luggage as they exit the premise. Permission for this search is granted by the Visitor signature on the Visitor Agreement Form (see the Check-In section of this document).

5.8 Emergency Evacuation

In the event of an emergency, it is the sponsoring employee's responsibility to ensure that the Visitor remains in the Evacuation marshaling area.

Emergency Coordinators will tally all Visitors using the Visitor Check-In information (using either the preferred online method or the fall-back paper sheets). Visitors will not leave the property until it is confirmed with the Emergency Coordinators that they have successfully evacuated the building.

5.9 Multiple Day Visits and Longer Term Contracts

Visitors who are at Commercial Connect LLC for multiple days must follow all procedures associated with this policy (Check-In, Check-Out, etc.) on each day of their visit. Longer term contractors can be sponsored for a photo-ID badge and would then fall under the Long Term Contractor Policy.

5.10 Visitors and Groups Requesting Tours of the Facility

All requests by groups for tours of Commercial Connect LLC facility will be referred to the Human Resources Department and/or the Office of the CSO for handling as an exception. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative.

In these cases, a verbal summary of the Emergency Evacuation Procedure and the restrictions on Photographs will be communicated to the Visitor Group prior to entry of the facility by a pre-designated Commercial Connect LLC employee. Any hazard specific to the areas being visited will also be communicated at that time. Visits to areas of this type may require waivers to be signed individually before entry to the facility.

All Visitors or Groups on a tour will be accompanied by their sponsor(s) at all times.

5.11 Network or System Access

Consultants or other Visitors that require internet network access can freely access the Visitor Wireless Network. Access to this network requires on-line agreement to the terms and conditions of network use. The unique number on the back of the Visitor badge is required to authenticate on the web page that is presented on access to this network.

Visitors who require access to production IT networks will need permission from their employee sponsor, who will arrange temporary credentials with the Helpdesk. Part of this procedure will require the Visitor to review the Acceptable Use Policy. *After credentials are arranged, activities on the network will be subject to the Acceptable Use Policy. Visitor use of employee credentials is not permitted under any circumstances.*

Visitors who require access to the production PLC or SCADA network will require prior permission from the Plant Manager and the Office of the CSO. Visitor use of employee credentials is not permitted under any circumstances.

Contractors making changes to production systems on either the IT or PLC/SCADA networks are subject to the IT and Production Systems Change Control Policy. In these cases, employee sponsors are required to review this policy with affected Visitors and ensure that the lead time and exceptions sections especially are clearly identified.

Remote Access to Commercial Connect LLC networks are governed by the Commercial Connect LLC Remote Access Policy.

5.12 On Courtesy

All employees of Commercial Connect LLC are to bear in mind at all times that all Visitors are either Customers or potential Customers. Even in the case of clear violations of this policy, all actions, dealings and conversations are to be courteous in nature.

6.0 Responsibility

This document is maintained jointly by the Human Resources Department and the Office of the CSO (Chief Security Officer).

Enforcement of this policy falls to these offices, as indicated in this document

Administration of the Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. In most facilities it is a duty of the main Reception Desk.

7.0 Penalties

Violation of any of the requirements in this policy by any employee will result in suitable disciplinary action, up to and including prosecution and / or termination.

Violation of any of the requirements in this policy by any Visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

8.0 Related Documents

The following documents are referenced in this policy. It is the responsibility of employees sponsoring Visitors to Commercial Connect LLC to ensure that Visitors are compliant with all policies and procedures that apply to any activities and situations that occur while on-site. In some cases Visitors to Commercial Connect LLC may be asked to review, agree to, and in some cases sign one or more of these documents as part of their Check-In process.

- *Visitor Check-In Procedure*
- *Visitor Check-In Agreement*
- *Laptop, Computer and related equipment Check-In / Check-out Procedure*
- *Emergency Evacuation Policy*
- *Emergency Evacuation Procedures (Note that this encompasses several documents)*
- *Visitor Network Access Agreement (online webpage, a paper copy of this agreement under revision control is maintained by and available from the Office of the CSO)*
- *IT and Production Systems Change Control Policy*
- *Network User Registration Policy*
- *Network User Registration Procedure*
- *Computer and Network Acceptable Use Policy*
- *Remote Access Policy*

All Corporate Policies and Procedures are to be considered confidential information. While many of these Corporate Documents are required by Visitors as part of their visit, any policies or procedures not required in this capacity should be considered to be governed by the "Information Disclosure" section of this document.

9.0 Revision History

Version 1.0 – Rob VandenBrink	*Date: 24 March 2010* *Initial Version*

Wireless Communication Policy

Overview

The purpose of this policy is to secure and protect the information assets owned by Commercial Connect LLC. Commercial Connect LLC provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Commercial Connect LLC grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Commercial Connect LLC network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a Commercial Connect LLC network.

Scope

All employees, contractors, consultants, temporary and other workers at Commercial Connect LLC, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Commercial Connect LLC must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Commercial Connect LLC network or reside on a Commercial Connect LLC site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

The Information Security Department must approve exceptions to this policy in advance.

Policy Statement

General Network Access Requirements

All wireless infrastructure devices that reside at a Commercial Connect LLC site and connect to a Commercial Connect LLC network, or provide access to information classified as Commercial Connect LLC Confidential, Commercial Connect LLC Highly Confidential, or Commercial Connect LLC Restricted must:

Abide by the standards specified in the Wireless Communication Standard.

Be installed, supported, and maintained by a approved support team.

Use Commercial Connect LLC approved authentication protocols and infrastructure.

Use Commercial Connect LLC approved encryption protocols.

Maintain a hardware address (MAC address) that can be registered and tracked.

Not interfere with wireless access deployments maintained by other support organizations.

Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to Commercial Connect LLC Confidential, Commercial Connect LLC Highly Confidential, or Commercial Connect LLC Restricted information must adhere to section 0. Lab and isolated wireless devices that do not provide general network connectivity to the Commercial Connect LLC network must:

Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the DMZ Lab Security Policy or the Internal Lab Security Policy.

Not interfere with wireless access deployments maintained by other support organizations.

Home Wireless Device Requirements

Wireless infrastructure devices that provide direct access to the Commercial Connect LLC corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Commercial Connect LLC corporate network. Access to the Commercial Connect LLC corporate network through this device must use standard remote access authentication.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Commercial Connect LLC.

Definitions

Term	Definition
Commercial Connect LLC network	*A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.*
Corporate connectivity	*A connection that provides access to a Commercial Connect LLC network.*
Enterprise Class Teleworker (ECT)	*An end-to-end hardware VPN solution for teleworker access to the Commercial Connect LLC network.*
Information assets	*Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.*
MAC address	*The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.*

Revision History

Date of Change	Responsible	Summary of Change