Internet & E-Mail Acceptable Use Policy

Expectation of privacy:

Any employees of this company can have NO expectation of privacy concerning email, phone, IM, Text messaging, web browsing or data when using company resources. That includes, but is not limited to:

- Company email
- Company Internet connection
- Company computers (notebook and desktop)
- Company phone services
- Company data network
- Company server(s)
- Company premises

Acceptable uses of the Internet and company e-mail:

Use of the company provided Internet and e-mail access is intended to be for business reasons only. The company encourages the use of the Internet and e-mail because they make communication more efficient and effective. However, Internet service and e-mail are company property, and their purpose is to facilitate company business. Every staff member has a responsibility to maintain and enhance the company's public image and to use company e-mail and access to the Internet in a productive manner. To ensure that all employees are responsible, the following guidelines have been established for using e-mail and the Internet. Any improper use of the Internet or e-mail is not acceptable and will not be permitted.

Unacceptable uses of the Internet and company e-mail:

The company e-mail and Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or Pornographic. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted through the company's e-mail or Internet system. Electronic media may also not be used for any other purpose that is illegal or against company policy or contrary to the company's best interest. Solicitation of non-company business or any use of the company e-mail or Internet for personal gain is prohibited. The use of Company email for any personal use like non work related website registration is also prohibited as this greatly increases the chance of company email details being intercepted and misused by third parties.

Communications:

Each employee is responsible for the content of all text, audio or images that they place or send over the company's e-mail/Internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else or someone from another company. All messages communicated on the company's e-mail/Internet system should contain the employee's name. Any messages or information sent by an employee to another individual outside of the company via

an electronic network (e.g., bulletin board, on-line service or Internet) are statements that reflect the company. While some users include personal "disclaimers" in electronic messages, there is still a connection to the company, and the statements may be tied to the company. All communications sent by employees via the company's e-mail/Internet system must comply with this and other company policies and may not disclose any confidential or proprietary company information.

Software:

To prevent computer viruses from being transmitted through the company's e-mail/Internet system, there will be no unauthorized downloading of any unauthorized software. All software downloaded must be registered to the company. Employees should contact Management if they have any questions.

Copyright Issues:

Copyrighted materials belonging to entities other than this company, may not be transmitted by employees on the company's e-mail/Internet system. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, expect with permission, or as a single copy to reference only. Failure to observe copyright or license agreements may result in disciplinary action up to and including termination.

Security:

The Company routinely monitors usage patterns for its e-mail/Internet communications. The reasons for this monitoring are many, including cost analysis/allocation and the management of the company's gateway to the Internet. All messages created sent, or retrieved over the company's e-mail/Internet are the property of the company and should be considered public information. The company reserves the right to access and monitor all messages and files on the company's e-mail/Internet system as deemed appropriate. Employees should therefore, not assume electronic communications are totally private and should transmit highly confidential data in other ways.

Violations:

Any employee found to be abusing the privilege of company facilitated access to e-mail or the Internet, will be subject to corrective action up to and including termination. If necessary, the company also reserves the right to advise appropriate legal officials of any illegal violations.

E-MAIL/INTERNET USER AGREEMENT

Employee Agreement:

I have received a copy of the CJA Telecommunications Corporate Policy Guideline on e-mail/Internet acceptable use. I recognize and understand that the company's e-mail/Internet systems are to be used for conducting the company's business only. I understand that use of this equipment for private purposes is strictly prohibited.

As part of the CJA Telecommunications organization and user of CJA Telecommunications' gateway to the Internet and e-mail system, I understand that this e-mail/Internet corporate guideline applies to me.

I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment with CJA Telecommunications.

I am aware that violations of this corporate guideline on e-mail/Internet acceptable use may subject me to disciplinary action, up to and including discharge from employment.

I further understand that my communications on the Internet and e-mail reflect CJA Telecommunications, world-wide to our competitors, consumers, customers and suppliers. Furthermore, I understand that this document can be amended at any time.

Company Laptop and Electronic Device Usage Policy

Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at CJA Telecommunications in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

CJA Telecommunications provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

Scope

All employees, contractors, consultants, temporary and other workers at CJA Telecommunications, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by CJA Telecommunications, or to devices that connect to a CJA Telecommunications network or reside at a CJA Telecommunications site.

Information Security must approve exceptions to this policy in advance through a request in writing to any managerial staff member.

Policy Statement

General Requirements

You are responsible for exercising good judgment regarding appropriate use of CJA Telecommunications resources in accordance with CJA Telecommunications policies, standards, and guidelines. CJA Telecommunications resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices

or users on the CJA Telecommunications network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

1. System Accounts

You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

You must maintain system-level and user-level passwords in accordance with the Password Policy.

You must ensure through legal or technical means that proprietary information remains within the control of CJA Telecommunications at all times. Conducting CJA Telecommunications business that results in the storage of proprietary information on personal or non- CJA Telecommunications controlled environments, including devices maintained by a third party with whom CJA Telecommunications does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by CJA Telecommunications, or its customer and partners, for company business.

2. Computing Assets

You are responsible for ensuring the protection of assigned CJA Telecommunications assets that includes the use of computer cable locks and other security devices. Laptops left at CJA Telecommunications overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of CJA Telecommunications assets to Management.

All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Devices that connect to the CJA Telecommunications network must comply with the Minimum Access Policy.

Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, Anti-Malware, and Firewall.

3. Network Use

You are responsible for the security and appropriate use of CJA Telecommunications network resources under your control. Using CJA Telecommunications resources for the following is strictly prohibited:

Causing a security breach to either CJA Telecommunications or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

Causing a disruption of service to either CJA Telecommunications or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

Introducing honeypots, honey nets, or similar technology on the CJA Telecommunications network.

Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

Use of the Internet or CJA Telecommunications network that violates the Internet and Email acceptable use policy, CJA Telecommunications policies, or local laws.

Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key loggers.

Port scanning or security scanning on a production network unless authorized in advance by Information Security.

4. Electronic Communications

The following are strictly prohibited:

Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates CJA Telecommunications policies against harassment or the safeguarding of confidential or proprietary information.

Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Use of a CJA Telecommunications e-mail or IP address to engage in conduct that violates CJA Telecommunications policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a CJA Telecommunications e-mail or IP address represents CJA Telecommunications to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

5. 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 CJA Telecommunications.

6. Definitions

Term	Definition
honeypot, honey net	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.