



JC-XX-xxxx Rev A

Internet Usage Policy

© Jamcracker, Inc., 2001 - Proprietary and Confidential

Effective: 09-01-01

Page 1 of 4

The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

1. Context

This policy applies to all company employees and all other authorized users of the global electronic mail and messaging infrastructure made available by the company, including Internet, intranet and on-line access provider systems. Users are responsible for complying fully with this policy as stated, but the company reserves the right to modify this policy at any time, with or without prior notification. Violations could be the basis for employee discipline or discharge.

2. General

Internet and intranet access, including electronic mail, is provided to employees as a business communication tool for appropriate internal and external business uses. Jamcracker's corporate e-mail system (the "system") is owned solely by the company and information in the system will be treated just like other company business records, files, electronic records, documents, materials and equipment. Prohibited uses of e-mail are detailed in section 3 of this policy. Users must take particular care not to disseminate confidential company information to unauthorized users, either directly or indirectly.

Use of the system for the communication of personal, private or confidential information is not appropriate. If incidental or occasional personal use of the system is made, such use is still subject to the same policies and procedures set out in this policy.

Jamcracker reserves the right to review all company electronic records, including e-mail messages. Therefore, employees should have no personal expectation that their electronic exchanges, including their mail messages, are private.

Because e-mail messages deleted by the user may still be present, either in another person's mailbox, or on a file server or back-up file (archives may be kept for at least six (6) months), care must be taken to ensure the accuracy and professionalism of all e-mail communications. E-mail messages must be able to withstand scrutiny without causing embarrassment to the company, its employees or customers.

All company policies — including but not limited to policies concerning copyright, confidentiality, harassment and compliance with equal



The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

employment laws — apply to the use of the Internet including, but not limited to, electronic mail.

3. Procedures and Guidelines

3.1. *Authorized Uses of Internet Connection*

All company employees with a legitimate business purpose may use the Internet connectivity. The intended use includes exchange of e-mail, web conferencing, information research and browsing, for work related purposes, as well as file exchanges. Other purposes may be suitable as well and must be approved by management and communicated to the Operations Department.

3.2. *Security of Confidential Messages and User Passwords*

1. Employees must ensure that internal messages meant only for company employees are not sent to outsiders.
2. Private and confidential information must be encrypted with strong encryption techniques before being transmitted to a valid party over any public network. Sending information by e-mail on the Internet is equivalent to sending a post card via regular mail, allowing anyone to view the information sent.
3. System users should secure access to their mailboxes using passwords and other security devices and should not leave the System on and available to unauthorized users.
4. Care must be taken as not to send any user IDs and passwords over any public network. Many Internet applications only allow such mechanism. In doubt, the user must consult with the Corporate Security Department before attempting to access any such application.
5. Internet, intranet and/or on-line access provider services and the company's Internet, intranet or service provider address may be used solely for business purposes.
6. Employees may not reveal any confidential internal e-mail names and passwords of other company employees to anyone outside of the company, including to people who request such information over the telephone and seem to have a legitimate reason for asking. All such requests must be referred to the System Administrators or to the Corporate Security Department for analysis and for an adequate response.
7. Extreme care must be taken in both configuration of the system and content of communications not to expose the company to risk of a security breach, harassment or sabotage.



The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

3.3. Prohibited Uses of Internet

Some uses of the Internet are prohibited at Jamcracker. These uses are:

- sending or downloading copies of documents in violation of copyright laws or licensing agreements;
- sending or downloading messages prohibited or restricted by government security laws or regulations;
- sending confidential or proprietary information or data to persons not authorized to receive it, either within or outside the company;
- sending content that may constitute sexual harassment or be considered discriminatory, obscene, derogatory or excessively personal, whether intended to be serious or humorous;
- downloading of material that may be considered discriminatory, obscene or pornographic;
- sending chain letters;
- engaging in illegal activity;
- harassment;
- exchanging sensitive information related to possible or actual litigation;
- carrying personal commercial activities;
- engaging in promotion of political positions or actions;
- solicitation of any type, except for company-sanctioned activities.

Employees cannot disclaim responsibility for failure to adhere to these restrictions. If you need clarification on any of these prohibited uses, contact the company's Legal Department or the Human Resources Department.

3.4. Privacy/Access to Electronic Mail

Jamcracker has the technical capabilities to monitor all network traffic, for problem diagnostic or other purposes, although it does not intend to routinely monitor the contents of electronic mail messages. Moreover, users should expect that electronic mail messages might be accessed by authorized supervisors or system administrators with or without the permission of the employee. However, no other employees may monitor network traffic or access e-mail messages of another user.

Any requests for access to the contents of e-mail in order to respond to legal process, such as subpoenas, or for purposes of representing the company in connection with any actual or threatened litigation, investigation or claim must be brought to the attention of the company's Legal Department.



The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

Unauthorized access of e-mail messages is a serious violation of company policy and grounds for dismissal.

3.5. Responsibilities

All employees must ensure that they have management authorization to use the Internet connection for any use that is not explicitly outlined in this document. All employees are responsible for adhering to this policy. Employees should notify the Legal, Corporate Security or HR Department of any violations of this policy.

Jamcracker's management and Department Heads are responsible for (a) ensuring that their employees understand this policy and for monitoring usage within their department; (b) ensuring that access privileges are terminated when appropriate in cases of transfer, termination or changes of assignment; and (c) cooperating with and providing resources for investigations of system use and misuse.

3.6. Stipulations for e-mail

All employees must be aware of the following when using e-mail:

- E-mail messages can be misdirected by the sender or by an error in the message routing process.
- E-mail relies on public networks that are outside company control. Service levels and confidentiality cannot be guaranteed. Once sent, e-mail messages cannot always be retrieved or removed from a recipient's mailbox.
- E-mail messages sent across the Internet are inherently easy to forge or modify. When in doubt about the authenticity or the integrity of a message, recipient of message must take alternative actions¹ to verify the accuracy of the contents and the authenticity of its originator.

¹ Such actions include a telephone call, paying a visit, or any other mean except use of the e-mail system suspected of being compromised.