

# Acceptable Use Policy

## A framework for e-mail and Internet usage policies for COMPANY

### E-mail security policy

#### **Purpose**

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.

#### **Scope**

The policies apply to COMPANY employees and contractors and cover e-mail located on COMPANY personal computers and servers if these systems are under the jurisdiction and/or ownership of COMPANY. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.

#### **Specific policy**

**Company property.** As a productivity enhancement tool, COMPANY encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of COMPANY, and are not the property of users of the electronic communications services.

# Acceptable Use Policy

**Authorized usage.** COMPANY electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:

- (a) It does not consume more than a trivial amount of resources.
- (b) It does not interfere with staff productivity.
- (c) It does not preempt any business activity.

Users are forbidden from using COMPANY electronic communications systems for charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by the COMPANY Owners or representatives. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

**Default privileges.** Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of a program director has been obtained.

**User separation.** These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. But fax machines that do not have separate mailboxes for different recipients need not support such user separation. All COMPANY staff and authorized contractors have unique usernames and passwords to access the e-mail system.

**User accountability.** Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password.

If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

**No default protection.** Employees are reminded that COMPANY electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. See Arno D Joubert if this requirement is needed.

**Respecting privacy rights.** Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. COMPANY is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

However, COMPANY also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

# Acceptable Use Policy

**No guaranteed message privacy.** COMPANY cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

**Regular message monitoring.** It is the policy of COMPANY NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that COMPANY will from time to time examine the content of electronic communications.

**Statistical data.** Consistent with generally accepted business practice, COMPANY collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, Information Systems (IS) staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.

**Incidental disclosure.** It may be necessary for IS staff to review the content of an individual employee's communications during the course of problem resolution. IS staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels (Director, Ops Manager, etc.).

**Message forwarding.** Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. COMPANY's sensitive information must not be forwarded to any party outside COMPANY without the prior approval of Arno D Joubert or the COMPANY Director. Blanket forwarding of messages to parties outside COMPANY is prohibited unless the prior permission of Arno D Joubert or the Director has been obtained.

**Purging electronic messages.** Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period—generally six months—electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by IS staff.

Not only will this increase scarce storage space; it will also simplify record management and related activities. If COMPANY is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the COMPANY Director or his designated representative has communicated that it is legal to do so.

## Responsibilities

As defined below, COMPANY groups and staff members responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility.

1. COMPANY must establish e-mail security policies and standards and provide technical guidance on e-mail security to all COMPANY staff.
2. COMPANY staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Section Managers must ensure that their staffs are in compliance with the personal computer security policy established in this document. COMPANY

# Acceptable Use Policy

staff must also provide administrative support and technical guidance to management on matters related to e-mail security.

3. COMPANY Section Managers must ensure that:

- Employees under their supervision implement e-mail security measures as defined in this document.

## **Contact point**

Questions about this policy may be directed to Arno D Joubert.

## **Disciplinary process**

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

## **Internet Security Policy**

### **Purpose**

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of COMPANY information and equipment by Internet connections.

### **Scope**

This policy applies to all employees, contractors, consultants, temporaries, and other users at COMPANY, including those users affiliated with third parties who access COMPANY computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by COMPANY.

### **Specific policy**

All information travelling over COMPANY computer networks that has not been specifically identified as the property of other parties will be treated as though it is a COMPANY corporate asset. It is the policy of COMPANY to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of COMPANY to protect information belonging to third parties that has been entrusted to COMPANY in confidence as well as in accordance with applicable contracts and industry standards.

### **Introduction**

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes COMPANY's official policy regarding Internet security. It applies to all users (employees, contractors, temporaries, etc.) who use the Internet with COMPANY computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with COMPANY.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to Arno D Joubert. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

# Acceptable Use Policy

## Information movement

All software downloaded from non-COMPANY sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.

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

Unless tools like privacy enhanced mail (PEM) are used, it is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with COMPANY information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal COMPANY information (see the following section).

Users must not place COMPANY material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the Owners have first approved the posting of these materials.

In more general terms, COMPANY internal information should not be placed in any location, on machines connected to COMPANY internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly writable (common/public) directories on COMPANY Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with COMPANY's business.

Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

## Information protection

Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, COMPANY secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Credit card numbers, bank account details, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. The PGP (pretty good privacy) encryption algorithm, or another algorithm approved by COMPANY, must be used to protect these parameters as they traverse the Internet.

This policy does not apply when logging into the machine that provides Internet services. Currently COMPANY does not use any type of encryption.

In keeping with the confidentiality agreements signed by all staff, COMPANY software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-COMPANY party for any purposes other than business purposes expressly authorized by management.

Exchanges of software and/or data between COMPANY and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

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 that is not consistent with the vendor's license is strictly forbidden.

# Acceptable Use Policy

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with COMPANY work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

## **Expectation of privacy**

Staff using COMPANY information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private.

At any time and without prior notice, COMPANY management reserves the right to examine e-mail, personal file directories, and other information stored on COMPANY computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of COMPANY information systems.

## **Resource usage**

COMPANY management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not company, time. Likewise, games, news groups, and other nonbusiness activities must be performed on personal, not company, time.

Use of COMPANY computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is preempted by the personal use. Extended use of these resources requires prior written approval by a director.

## **Public representations**

Staff may indicate their affiliation with COMPANY in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.

In either case, whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of COMPANY.

All external representations on behalf of the company must first be cleared with the director of marketing or Owners. Additionally, to avoid libel problems, whenever any affiliation with COMPANY is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

Staff must not publicly disclose internal COMPANY information via the Internet that may adversely affect COMPANY's customer relations or public image unless the approval of the Marketing Manager or Director has first been obtained. Such information includes business prospects, unit costing, RFP information, and the like. Responses to specific customer e-mail messages are exempted from this policy.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If staff aren't careful they may let the competition know that certain internal projects are underway. If a user is working on an unannounced product, a research and development project, or related confidential COMPANY matters, all related postings must be cleared with one's line manager and Director prior to being placed in a public spot on the Internet.

## **Access control**

All users wishing to establish a connection with COMPANY computers via the Internet must authenticate themselves at a firewall before gaining access to COMPANY's internal network. This authentication process must be done via a dynamic password system approved by the Operations Manager.

Examples are handheld smart cards or user-transparent challenge/response. This will prevent intruders from guessing passwords or from replaying a password captured via a "sniffer attack" (wiretap).

# Acceptable Use Policy

Designated "public" systems do not need these authentication processes because anonymous interactions are expected. Currently, COMPANY does not use this system.

Unless the prior approval of the CIO has been obtained, staff may not establish Internet or other external network connections that could allow non-COMPANY users to gain access to COMPANY systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet home pages, FTP servers, and the like.

Likewise, unless the Operations Manger, Marketing Manager, Director, and legal counsel have all approved the practice in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with online shopping, online database services, etc.

## Reporting security problems

If sensitive COMPANY information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Operations Manager must be notified immediately.

If any unauthorized use of COMPANY's information systems has taken place, or is suspected of taking place, the Operations Manager must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Operations Manager must be notified immediately.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not "test the doors" (probe) security mechanisms at either COMPANY or other Internet sites unless they have first obtained permission from the Operations Manager. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

## Responsibilities

As defined below, COMPANY groups and staff members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

a) COMPANY must establish Internet security policies and standards and provide technical guidance on PC security to all COMPANY staff. COMPANY must also organize a computer emergency response team (CERT) to respond to virus infestations, hacker intrusions, and similar events. The CERT Team is identified in COMPANY's Personal Computer Security Policy.

b) COMPANY' staff must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Section Managers must ensure that their staffs are in compliance with the Internet security policy established in this document. COMPANY staff must also provide administrative support and technical guidance to management on matters related to Internet security.

c) IS staff must periodically conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.

d) COMPANY staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

e) COMPANY staff must check that user access controls are defined on these systems in a manner consistent with the need-to-know.

f) COMPANY information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

g) COMPANY Section Managers must ensure that:

1. Employees under their supervision implement security measures as defined in this document.

# Acceptable Use Policy

2. Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
3. Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all COMPANY documents that address information security.
4. Employees and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.
5. Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

h) Users of COMPANY Internet connections must:

- 1) Know and apply the appropriate COMPANY policies and practices pertaining to Internet security.
- 2) Not permit any unauthorized individual to obtain access to COMPANY Internet connections.
- 3) Not use or permit the use of any unauthorized device in connection with COMPANY personal computers.
- 4) Not use COMPANY Internet resources (software/hardware or data) for other than authorized company purposes.
- 5) Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
- 6) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
- 7) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
- 8) Report to COMPANY any incident that appears to compromise the security of COMPANY information resources. These include missing data, virus infestations, and unexplained transactions.
- 9) Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
- 10) Obtain supervisor authorization for any uploading or downloading of information to or from COMPANY multi-user information systems if this activity is outside the scope of normal business activities.
- 11) Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by their section manager.

## **Contact point**

Questions about this policy may be directed to the Owners.

## **Disciplinary process**

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.