



Internet Acceptable Usage Policy Guidelines

Contents

SUMMARY INTERNET USAGE POLICY PROVISIONS.....	3
INTERNET USAGE POLICY.....	3
Overview	3
DETAILED INTERNET USAGE POLICY PROVISIONS	4
A) General	4
B) Technical.....	5
C) Security	5
Acknowledgment	5

SUMMARY INTERNET USAGE POLICY PROVISIONS

1. Vision AfriKa has software and systems in place that can monitor and record all Internet usage.
2. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.
3. Sexually explicit material may not be accessed, displayed, archived, stored, distributed, edited or recorded using our network or computing resources.
4. Use of any Vision AfriKa resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.
5. Any software or files downloaded via the Internet into Vision AfriKa network become the property of Vision AfriKa.
6. No employee may use Vision AfriKa facilities knowingly to download or distribute pirated software or data.
7. No employee may use Vision AfriKa Internet facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code.
8. In the interest of keeping Vision AfriKa well-informed, use of news briefing services like Pointcast is acceptable.
9. Employees with Internet access may not use Vision AfriKa Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
10. Employees with Internet access may not upload any software licensed to Vision AfriKa or data owned or licensed by Vision AfriKa without explicit authorization from the manager responsible for the software or data. The entire Internet Acceptable Usage Policy is attached to this document. Please read the policy and return the Acknowledgment to Human Resources.

INTERNET USAGE POLICY

Overview

Vision AfriKa provides access to the vast information resources of the Internet to help you do your job and be well-informed. The facilities that provide access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. This Internet Acceptable Usage Policy is designed to help you understand the expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely. While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost, the Internet for this Vision AfriKa is a tool, provided to you at significant cost. That means we expect you to use your Internet access primarily for programme-related purposes, i.e., to research relevant topics and obtain useful information (except as outlined below). We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all existing Vision AfriKa policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of Vision AfriKa resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the organisation and expose the organisation to significant legal liabilities. Access to electronic communications gives each individual Internet user an immense and unprecedented reach to propagate Vision AfriKa messages and tell our business story.

Because of that power, one must take special care to maintain the clarity, consistency and integrity of the Vision AfriKa image and posture. Anything any one employee writes in the course of acting for Vision AfriKa on the Internet could be taken as representing Vision AfriKa posture. That is why we expect you to forego a measure of your individual freedom when you participate in electronic communications as outlined below. While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features. The overriding principle is that security is to be everyone's first concern. Vision AfriKa employees can be held accountable for any breaches of security or confidentiality including any and all branches. "Document" covers just about any type of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. "Graphics" includes photographs, pictures, animations, movies or drawings. "Display" includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions, and virtual-reality tools.

DETAILED INTERNET USAGE POLICY PROVISIONS

A) General

1. Vision AfriKa has software and systems in place that monitor and record all Internet usage. Our security systems are capable of recording (for each and every user) each World Wide Web site visit and each email message into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. Our managers will review Internet activity and analyse usage patterns and they may choose to publicize this data to assure that Vision AfriKa internet resources are devoted to maintaining the highest levels of productivity.
2. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.
3. The display of any kind of sexually explicit image or document on any Vision AfriKa system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be accessed, archived, stored, distributed, edited, or recorded using our network or computing resources.
4. Vision AfriKa uses independently-supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of.
If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately and report the matter to your manager, regardless of whether that site had been previously deemed acceptable by any screening or rating program.
5. Vision AfriKa Internet facilities and computing resources must not be used to violate the laws and regulations of South Africa or any other nation, or the laws and regulations of any province, city or other local jurisdiction in any material way. Use of any Vision AfriKa resources for illegal activity is grounds for immediate dismissal and we will cooperate with any legitimate law enforcement activity.
6. Any software or files downloaded via the Internet into Vision AfriKa network become the property of Vision AfriKa. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
7. No employee may use Vision AfriKa facilities to download or distribute pirated software or data.
8. No employee may use Vision AfriKa Internet facilities to propagate any virus, worm, Trojan horse or trap-door program code.
9. Each employee using the Internet facilities of Vision AfriKa shall identify himself or herself honestly, accurately and completely, when setting up accounts on outside computer systems.
10. Only those employees or officials who are authorized to speak to the media, to analysts or at public gatherings on behalf of Vision AfriKa may speak/write in the name of Vision AfriKa in any electronic communications. Where an individual participant is identified as an employee or agent of Vision AfriKa the employee must refrain from any political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by Vision AfriKa of any commercial product or service not sold or serviced by Vision AfriKa, its subsidiaries or its affiliates.
11. Vision AfriKa retains the copyright to any material posted on the Internet by any employee in the course of his or her duties.
12. Employees are reminded that it is inappropriate to reveal confidential information, and any other material covered by existing Vision AfriKa secrecy policies and procedures on the Internet. Employees releasing such confidential information— whether or not the release is inadvertent — will be subject to the penalties provided in existing Vision AfriKa policies and procedures.
13. Use of Vision AfriKa Internet access facilities to commit infractions such as misuse of Vision AfriKa assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are also prohibited by general Vision AfriKa policy and will be sanctioned under the relevant provisions of the personnel handbook.
14. Because a wide variety of materials may be considered offensive by colleagues, constituents or suppliers, it is a violation of Vision AfriKa policy to store, view, print, or redistribute any document or graphic file that is not directly related to the user's job or Vision AfriKa activities.
15. In the interest of keeping employees well-informed, use of news briefing services like Pointcast is acceptable, within limits that may be set by each department's activities.
16. Employees may use their Internet facilities for non-business research or browsing during meal time or other breaks, or outside of work hours, provided that all other usage policies are adhered to.
17. Employees with Internet access must take particular care to understand the copyright, trademark, libel, slander, and public speech control laws of all countries in which this governmental organisation maintains a business presence, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.
18. Employees with Internet access may not use Vision AfriKa Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
19. Employees with Internet access may not use Vision AfriKa Internet facilities to download images or videos unless there is an express business-related use for the material.
20. Employees with Internet access may not upload any software licensed to Vision AfriKa or data owned or licensed by Vision AfriKa without the express authorization of the manager responsible for the software or data.

B) Technical

1. User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource from Vision AfriKa must keep that password confidential. Vision AfriKa policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.
2. Employees should schedule communications -intensive operations such as large file transfers, video downloads, mass e-mailings and the like, for off-peak times.
3. Any file that is downloaded must be scanned for viruses before it is run or accessed.

C) Security

1. Vision AfriKa has installed an Internet firewall to assure the safety and security of the organisation's networks. Any employee who attempts to disable, defeat, or circumvent any security facility will be subject to immediate dismissal.
2. Files containing sensitive Company data, as defined by existing data security policy, that are transferred in any way across the Internet must be encrypted.
3. Only those Internet services and functions with documented business purposes for this organisation will be enabled at the Internet firewall.

Acknowledgment

I acknowledge that I have received a written copy of the Internet Acceptable Usage Policy for Vision AfriKa.

I understand the terms of this policy and agree to abide by them. I realize that the Vision AfriKa security software may record and store for management use the electronic email messages I send and receive, the Internet address of any site that I visit and any network activity in which I transmit or receive any type of file. I understand that any violation of this policy could lead to my dismissal from employment or even criminal prosecution. If you have any question regarding this policy or any situation not specifically addressed in this policy, see your supervisor or Vision AfriKa Personnel Director. This policy is subject to revision. Vision AfriKa will adequately post revisions, but it is the user's responsibility to ensure that his/her use of Vision AfriKa computing and communication resources conforms to current policy.

Signature

Name (Printed)

Date