claysys

ACCEPTABLE USE POLICY

CLAYSYS TECHNOLOGIES

Scanned by TapScanner

claysys

Revision History

Date	Version	Description
02.01.2020	1.0	Release version

Scanned by TapScanner

Contents

1. Network Acceptable Use Policy 4
1.1 General Use and Ownership 4
1.2 Security and Proprietary Information 5
1.3 Unacceptable Use 5
1.3.1 System and Network Activities 6
1.3.2 Email and Communications Activities 7

© ClaySys Technologies

Scanned by TapScanner

1. Network Acceptable Use Policy

ClaySys Technologies is committed to protecting all employees, clients and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet-related systems, including but not limited to computers, laptops, tablets, PDAs, wireless technology, operating systems, applications, removable electronic media, network accounts providing electronic mail, Internet browsing, and remote access, are the property of ClaySys Technologies. These resources are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every ClaySys Technologies employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This policy applies to all employees at ClaySys Technologies. This policy applies to all equipment, networks, systems, software and other resources owned or leased by ClaySys Technologies.

1.1 General Use and Ownership

1. While the IT Department desires to provide a reasonable level of privacy, employees should be aware that the data they create on the corporate systems remains the property of ClaySys Technologies. Because of the need to protect the network, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to ClaySys Technologies.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. ClaySys Technologies equipment, systems, email address, etc. are not to be used to pursue outside business activities not sanctioned by the company.
4. The IT Department recommends that any information that users consider sensitive or vulnerable be encrypted.
5. For security and network maintenance purposes, authorized individuals within ClaySys Technologies may monitor equipment, systems and network traffic at any time.
6. ClaySys Technologies reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

© ClaySys Technologies

Scanned by TapScanner

1.2 Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorized access to confidential information. Examples of confidential information include but are not limited to: credit card information, corporate strategies, trade secrets, specifications, employee, client, and research data.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed according to the Password Policy.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or locking them when the host will be unattended.
5. Use encryption of information when appropriate.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised.
7. Postings by employees from a ClaySys Technologies email address to technical forums should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ClaySys Technologies.
8. All hosts used by the employee that are connected to the ClaySys Technologies Internet/Intranet, whether owned by the employee or ClaySys Technologies, shall be continually executing approved virus-scanning software with a current virus database.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses and/or other malware.

1.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of ClaySys Technologies authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing company-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

© ClaySys Technologies

Scanned by TapScanner

claysys

1.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ClaySys Technologies.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ClaySys Technologies or the end user does not have an active license is strictly prohibited
3. Downloading and/or installing any type of software not related to job functions or not authorized by the IT Department.
4. Connecting network devices such as wireless access points or personal laptops into the ClaySys Technologies network environment without proper authorization from the IT Department.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a ClaySys Technologies computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any ClaySys Technologies account.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless authorized by the IT Department.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

© ClaySys Technologies

Scanned by TapScanner

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.
16. Providing information about, or lists of, ClaySys Technologies employees to parties outside ClaySys Technologies without written approval of management.

1.3.2 Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

1. Sending, forwarding or requesting email with any type of confidential data such as credit card data. Any exceptions must be approved by the IT Department
2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within ClaySys Technologies' s networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by ClaySys Technologies or connected via ClaySys Technologies' network.
8. Sending or forwarding email that is likely to contain computer viruses.
9. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam)

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

Ron Roy

Employee Name

Employee Signature

Date 19/08/22

© ClaySys Technologies

Scanned by TapScanner