

Computing and Communication Policy on Acceptable Use of Electronic Resources

Summary

This policy defines the boundaries of "acceptable use" of electronic resources, including computers, networks, electronic mail services and electronic information sources, as detailed below. It includes by reference a self-contained compilation of specific rules that can be modified as the electronic information environment evolves.

The policy is based on the principle that the electronic information environment is provided to support Stone India's business and its vision to pursue and consolidate its position of leadership through passion, innovation and teamwork. Other uses are secondary. This policy prohibits uses that threaten the integrity of the system; the function of unauthorised equipment that can be accessed through the system; the privacy or actual or perceived safety of others; or that are otherwise illegal are forbidden.

By using the Organization's information systems you assume personal responsibility for their appropriate use and agree to comply with this policy as detailed below.

The policy defines penalties for infractions, up to and including loss of system access, employment termination or expulsion and / or other disciplinary action deemed fit by the company. In addition, some activities may lead to risk of legal liability, both civil and criminal, for which, you shall be solely responsible.

Users of electronic information systems are urged, in their own interest, to review and understand the contents of this policy.

Purposes

Stone India Limited makes computing resources (including, but not limited to, computer facilities and services, computers, networks, electronic mail, electronic information and data, voice services, and any such services which will be available in future) available to its employees, registered guests and other approved users in order to fulfill the vision and mission objectives of the company while undertaking its day to day business.

When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced. Authorized systems personnel may set and alter priorities for exclusively local computing/networking resources. The priorities for use of computing resources are:

Highest: Uses that directly support the business functionality of Stone India Limited.

Medium: Other uses that indirectly benefit the training and education, research and service missions of the organization.

Lowest: Personal communication not linked anyway with the business functionality of the organization.

Forbidden: Recreation, including game playing, viewing of indecent, obscene or pornographic material. All other activities which violate the rules mentioned in this policy.

The company may enforce these priorities by restricting or limiting usages of lower priority in circumstances where their demand and limitations of capacity impact or threaten to impact usages of higher priority.

Implied consent

Each person with access to the company's computing resources is responsible for their appropriate use and by their use agrees to comply with the company's computing & communication policies.

General Standards for the Acceptable Use of Computer Resources: Failure to uphold the following General Standards for the Acceptable Use of Computer Resources constitutes a violation of this policy and may be subject to disciplinary action.

The General Standards for the Acceptable Use of Computer Resources require:

- Responsible behavior with respect to the electronic information environment at all times;
- Behavior consistent with the mission and vision and code of business conduct & ethics of the company;
- Respect for the principles of open expression;
- Compliance with all applicable laws, regulations and company policies;

- Truthfulness and honesty in personal and computer identification;
- Respect for the rights and propriety of others, including intellectual property rights;
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and
- Respect for the value and intended use of human and electronic resources.

Enforcement and Penalties for Violation: Any person who violates any provision of this policy may face enquiry and disciplinary action as deemed fit by the company's management and/or as per clauses mentioned in IT Act, 2000. It may at times be necessary for authorized systems administrators to suspend someone's access to company's computing resources immediately for violations of this policy, pending interim resolution of the situation (for example by securing a possibly compromised account and/or making the owner of an account aware in person that an activity constitutes a violation). In the case of egregious and continuing violations suspension of access may be extended until final resolution by the appropriate disciplinary body.

System owners, administrators, managers or any other agency deemed appropriate by the Company may be required to investigate violations of this policy and to ensure compliance.

Amendment

Formal amendment of the General Standards of Acceptable Use of Computing Resources or other aspects of this policy may be made by a suitable committee as appointed by the company's management

Interpreting this policy

As technology evolves, questions will arise about how to interpret the general standards expressed in this policy. The Information & Technology Department in consultation with the Managing Director and other members of the Management Committee shall, after consultation with the legal cell of the company, publish specific rules interpreting this policy.

Waiver

When restrictions in this policy interfere with the research, educational or service missions of the company, employees of the company may request a written waiver from the Managing Director of the Company.

Specific Rules Interpreting the Policy on Acceptable Use of Electronic Resources

The following specific rules apply to all uses of the company's computing resources. These rules are not an exhaustive list of prescribed behaviors, but are intended to implement and illustrate the General Standards for the Acceptable Use of Computer Resources, other relevant company policies, and applicable laws and regulations.

Content of communications

- Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications (as defined by law), are prohibited.
- Communications containing information which may threaten the integrity of the organization or information pertaining to leakage of sensitive data of the company is prohibited.
- The use of computer resources for private business or commercial activities, fundraising or advertising, unauthorized use of the company's name, or any other use which is not connected with the operations or business of the Company are strictly prohibited.

Identification of users

The following activities and behaviors are prohibited:

- Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication;
- Acquiring or attempting to acquire passwords of others;
- Divulging or disclosing own passwords to others;
- Using or attempting to use the computer accounts of others;
- Alteration of the content of a message originating from another person or computer with intent to deceive; and

- The unauthorized deletion of another person's emails/documents.
- Unauthorized use of computer or electronic hardware allotted to or in the custody of another person.

Access to computer resources

The following activities and behaviors are prohibited:

- The use of computer resources or electronic information without or beyond one's level of authorization;
- The interception or attempted interception of communications by employees not explicitly intended to receive them;
- Making company computing resources available to individuals other than the staff of Stone India Limited without approval of an authorized official;
- Making available any materials the possession or distribution of which is illegal;
- The unauthorized copying or use of licensed computer software;
- Unauthorized access, possession, distribution or retention, by electronic or any other means, of electronic information or data that is confidential under the company's policies
- Intentionally compromising the privacy or security of electronic information; and
- Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).
- Unauthorized installation, modification, deletion of any software, screensavers, wallpapers which may hamper the performance of hardwares, softwares without the explicit authorization from authorized officials

Operational integrity

The following activities and behaviors are prohibited:

- Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts;

- Failure to comply with requests from appropriate authorized officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy;
- Revealing passwords or otherwise permitting the use by others (by intent, negligence or otherwise) of personal accounts for computer and network access;
- Altering or attempting to alter files or systems without authorization;
- Unauthorized scanning of networks for security vulnerabilities;
- Attempting to alter any company computing or networking components (including, but not limited to, bridges, routers, and hubs) without authorization or beyond one's level of authorization;
- Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;
- Intentionally damaging or destroying the integrity of electronic information;
- Intentionally disrupting the use of electronic networks or information systems;
- Intentionally mis-utilizing or wasting human or electronic resources; and
- Negligence leading to the damage of company's electronic information, computing/networking equipment and resources.