

Internet Acceptable Use Policy

Preface

The Internet Acceptable Use Policy (AUP) is part of a clearly communicated corporate strategy with Company employees. In an environment where users require freedom and flexibility in using Internet applications such as email and search, the AUP states and enforces a desired acceptable use – namely that the Internet is to be used to further the company’s business and improving customer service and not for personal entertainment or gain. All employees and contractors (the “staff”) of the Company Group (the “company”) are governed by this AUP.

1. Definitions

1.1. Digital assets

A digital asset is all computerized information that the company uses to compete or accomplish its mission. Examples of digital assets are:

- Customer Lists, Customer contracts, Terms and pricing in customer quotations
- Proprietary algorithms and methods of implementation
- Personally Identifiable Information of Employees
- Strategic marketing plans
- Documents marked as “Classified”

1.2. Ownership of digital assets

The company stakes claim to all digital assets generated, copied, processed, and stored by staff during the course of employ. This includes digital assets stored on personal workstations, hosted servers, office servers and transferred using an Internet communications channel.

1.3. Digital channels

Digital channels are a means of sending or receiving company messages, files and digital assets. Typical channels are:

- Email (SMTP, POP3)
- Web services, Web applications such as company Intranet
- Instant messaging, Text messaging, P2P applications such as Skype and Kazaa
- Flash drives

2. Acceptable use of PC and network

2.1. Physical Security

The staff is required to maintain and protect the physical security of digital assets, i.e. protecting mobile devices such as notebooks, PDA’s and cell-phones from being lost or stolen. For example – don’t put a notebook on an airport conveyor belt unattended or leave a PDA on your desk and go out to lunch.

2.2. Password security

The staff is responsible to maintain secrecy of workstation and server passwords. For example – passwords should not be written down on Post-IT™ notes stuck to a desk or PC. Passwords should be changed immediately if any staff feels that the secrecy is in question.

2.3. Personal activities

The company discourages the use of systems for personal activities.

2.4. Acceptable use of bandwidth

The staff will not use nor provide video streaming or peer-to-peer file sharing services. The staff will not upload nor download video files for personal use.

2.5. Privacy

Certain staff may have access to personal records of employees, customers, suppliers and business partners and will not leak or steal these digital assets.

3. Acceptable Use of digital channels

- **Email:** Be careful with the TO: and CC: fields in email. Email messages should not be forwarded to people who are not privy to the subject matter of the email. When sending email to distribution lists and groups in the company directory, make sure that the entire group needs to get the message.
- **Email attachments:** Delete email before reading from unknown Senders or email with attachments whose content or Subject is unfamiliar or unexpected.
- **Click here:** The staff will not download software or other content by clicking on a link on a Web site. If you need a particular software application, ask your supervisor.
- **Abusive content:** The staff will not be a willing originator of abusive or discriminatory content by mail, Web, IM or any other online channel.
- **Phishing:** Do not respond to emails asking you to click on a link in order to update personal account information. **Never** register at Web sites with your corporate email.
- **Data leakage:** The staff will not deliberately leak nor steal digital assets.

4. Enforcement

- The company reserves the right to terminate employment for any staff who violates this Acceptable Use Policy. Grounds for termination will be deliberate distribution of abusive content, deliberate leakage of digital assets without proper authorization, disclosure of information to a third party not constrained by a NDA (non-disclosure agreement), impersonating another person, aiding a hacker or initiating or participating in a denial of service attack.
- In order to enforce the AUP, the company may monitor digital channels.

Read and Understand Agreement

I hereby state that I have read and understood the Company Acceptable Use Policy and as a condition of my employment I agree to accept and abide by the principles, behavior and policies outlined.

EMPLOYEE SIGNATURE

MANAGER

DATE

DATE