



## Creating a Solid Acceptable Use Policy

By Mike Theriault  
President & CEO B2B Computer Products LLC

An Acceptable Use Policy (AUP) is a written document agreed to by everyone sharing a computer network. It defines the intended uses of the network including unacceptable uses and the consequences for violating the agreement. Although it may be necessary to include some legal terminology in the document, make an effort to put the AUP in clear terms that everyone can understand.

Before you start drafting the AUP, give notice to everyone affected that policy creation or revision is underway and establish a contact point for collecting feedback. Then decide on the purpose of your AUP. Will it only set general guidelines and expectations? Or will it be a legally enforceable document? This will have a strong bearing on the tone and wording.

### What an AUP Contains

Begin the document with your company's code of conduct, if you have one. Otherwise, develop a paragraph that sums up your company's operational ethics. While most companies will continually add to their AUP as issues arise, there are 10 basic areas that a solid AUP should cover.

1. Computer Security
2. Permitted Activities
3. Prohibited Activities
4. Social Media
5. Etiquette
6. Resource Use
7. Computer Vandalism & Harassment
8. The Level of Employee Privacy
9. Enforcement and Consequences for Noncompliance
10. Revisions and Updates

#### 1. Computer Security

Prohibit users from logging into any account other than their own, or allowing anyone else to log on with their credentials or use their systems when they are logged in. Consider adding language that:

- Requires employees to lock down workstations when away from their desks
- Addresses sending, receiving, and opening email attachments
- Prohibits users from disabling or working around computer security features
- Prohibits unauthorized software installation
- Prohibits unauthorized copying of company information to removable media, or sending it outside the network
- Defines computer vandalism
- Spells out exactly how employees should handle security problems that come to their attention

313 S. Rohlwing Road  
Addison, IL 60101  
p 630.396.6300  
tf 877.222.8857  
f 630.396.6322  
www.B2BComp.com

## 2. Permitted Activities

Avoid vague language and be very specific about what's allowed. Don't use words like "should" when you really mean "must". Don't use categories that can be misinterpreted such as "proprietary information". Instead list the categories of what is proprietary. Also spell out whether employees will be allowed limited personal use of corporate email accounts.

## 3. Prohibited Activities

Again, be very specific. Tackle such areas as:

- Sending, receiving, and downloading email, text, or images containing sexually explicit, pornographic, or offensive material
- Using the Web browser to visit online game or gambling sites or engage in any Internet activity that violates local, state or federal law – include the exact text of the most relevant regulations
- Sending an email, instant message, document, or other communication that discloses any confidential information about the company, its clients, or partners
- Soliciting - be sure employees know that the network cannot be used to solicit for any non-company-sponsored organization without prior written approval

## 4. Social Media

Employees need to know that creating a post with someone else's identity is illegal and that your company does not condone manipulating the social media conversation in any way. Other social media areas to consider include:

- **Access:** Spell out who has access to what. All employees don't need the same access to social media. For example, if marketing and sales are regularly creating posts and publishing videos, they'll need more leeway. However for those that deal with secure data, the social media policy must be more restrictive.
- **Ease of Use:** Strike a comfortable balance between personal use of social media and workplace productivity. Some companies impose a bandwidth-based limitation on social networking sites.
- **Downloading Software:** List only permissible software downloads and be very specific. Be clear that nothing else is allowed. If there isn't a pressing need for employees to download software from social media sites, don't allow it. In fact, consider blocking it.
- **Post-able Information:** Be clear as to what is inappropriate for employees to post to social networking sites. Also, be very specific about corporate proprietary information and confidential data. Confidences of present and former clients and employers should also be safeguarded. Be sure employees know not to comment on anything related to your company's legal matters or any pending litigation. Remind employees to protect their own privacy as well.

Employees must disclose any potential conflicts of interest – including any financial interest. Make it clear that employees should never use social media to knowingly mislead anyone including clients, fellow employees, or company officials.

## 5. Etiquette

Include language that encourages employees to email and post only meaningful, respectful remarks—in other words, no spam and nothing off-color, offensive, obscene, or harassing based on race, national origin, gender, sexual orientation, age, disability, religious belief or any other characteristic protected by federal, state and/or local law. When disagreeing with others, employees should be polite and appropriate – knowing that whatever they publish may be lingering on the Internet for a long time.

## 6. Resource Use

Be clear about what you will permit as far as attaching personally owned laptops, handheld computers, modems, wireless access points, and smart phones to the company network.

7. Computer Vandalism/Harassment

Define unacceptable activities – such as illegal file sharing; sending harassing or threatening content; sending spam; engaging in phishing; hacking into another system within or outside the network; distributing malicious code, accessing data on the network without permission; intercepting data on the network intended for others; and disguising email addresses or other network activity.

8. The Level of Employee Privacy

Be honest about any monitoring (active and passive) that may be occurring. Articulate the company's privacy policy regarding network users and include a statement that all communications stored on or sent to or from company computers or the company network may be monitored by the company for security purposes. Be sure employees know that the data they create on corporate systems remains the property of your company.

9. Enforcement and Consequences for Noncompliance

Spell out the penalties for AUP violations – including possible termination of employment. Be sure employees know that there may be civil and/or criminal penalties as well. Only set policies that you intend to apply equally and enforce.

10. Revisions and Updates

Include provisions for regular revisions, updates, and notifications. For example: *The content of this policy will be updated regularly to reflect new circumstances and applications as they arise. The most current AUP will always be posted on the company's intranet site.* Then establish a periodic update process for future revisions of the document.

Consider concluding the document with an FAQ section based on common questions and situations that actually occurred. Encourage employees to submit questions and use those as a basis for a continually evolving this section.

Create a rough outline of your AUP based on the information here, sample documents from other organizations similar to yours, and your own past experience. Publish the draft for the entire organization to read and comment on – collect feedback and make revisions. Have the final draft reviewed by legal counsel and then distribute the final AUP to everyone in your organization.

Hold brief meetings or webinars to clear up anything that employees don't understand and consider making Acceptable Use part of new hire training.

\*\*\*\*\*

About B2B Computer Products

Award-winning B2B Computer Products LLC was identified by *Inc.* magazine as one of the fastest growing businesses of its type in the U.S. and by *Crain's* as one of the largest privately held companies in the Chicago metro area. B2B Computer is a single-source provider of products and manufacturer-certified services that include virtualization, VoIP systems, data deduplication, disaster recovery, SAN storage, server consolidation, energy-efficiency improvement, and testing environment implementation. B2B Computer's engineers can design, configure, install, and/or manage the products and systems they sell to their clients. As a national business-to-business reseller of computer hardware and software representing hundreds of manufacturers – B2B guarantees a best practice combination of competitively priced customized products and expert services. In addition to its Addison, Illinois headquarters and multiple distribution points, B2B Computer's offices are in Chicago; New York; Davenport, Iowa; Philadelphia; and San Francisco. To contact B2B Computer, call 1-877-222-8857 or visit [www.B2BComp.com](http://www.B2BComp.com).