

# Websense® Mobile Acceptable Use Policy Kit

## **Mobile Acceptable Use Policy**

### CORPORATE SECURITY POLICIES

## \\nis202\Departments\Marketing\Collateral\TEMPLATES\WORD\WebsenseLogo_white_2in-01.png

|  |
| --- |
| Note: The content of this document is highly dependent on the current infrastructure and the degree to which you wish to support a Bring Your Own Device (BYOD) program in your organization. The policies listed herein are meant to serve as a best practice guideline reflective of those that are currently used in the mobile market.  All components of the policy below are highly applicable to the corporate device policy and can be modified accordingly to fit the elements of a BYOD policy. |

(Company Name) is hereinafter referred to as “the company”.

# Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this Acceptable Use Policy (AUP) is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user’s supervisor.

# Purpose

The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

# Scope

This policy applies to any and all use of corporate IT resources including, but not limited to, computer systems, personal mobile devices, email, network, and the corporate internet connection.

# Policy

## E-mail Use

Personal usage of company email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user’s job performance.

The information in this document should not be construed as legal advice or opinion and should not be considered representative of the views of Websense or its partners.  This document is not intended as a definitive statement on the subject matter addressed herein; rather, it is intended to serve as a tool providing practical reference for its readers.

* The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
* The user is prohibited from forging email header information or attempting to impersonate another person.
* Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption.
* It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.
* Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

## Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) posted on the Internet or any publicly accessible systems, or C) transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

## Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

## Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

* Engage in activity that is illegal under local, state, federal, international, or other applicable laws.
* Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
* Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
* Engage in activities that cause an invasion of privacy.
* Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
* Make fraudulent offers for products or services.
* Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of the employee’s job function.
* Install or distribute unlicensed or “pirated” software.
* Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

## Blogging

Blogging by the company’s employees is subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging is never allowed from the corporate computer network. In no blog, including blogs published from personal or public systems, shall the company be identified, company business matters be discussed, or material detrimental to the company be published. The user must not identify himself or herself as an employee of the company in a blog. The user assumes all risks associated with blogging.

## Instant Messaging

Instant Messaging is allowed for corporate communications only. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

## Web Browsing

The Internet is a network of interconnected computers of which the company has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet. The company recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user’s job performance.

## Copyright Infringement

The company’s computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CDs and DVDs; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which the employee has not already legally procured. This list is not meant to be exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above.

## Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.

## Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

## Expectation of Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

## Bandwidth Usage

Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage.

## Personal Usage

Personal usage of company computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the company or on the user’s job performance.

## Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

## Software Installation

While we cannot restrict users from installing software on their personal devices, extreme caution should be taken when installing any non-company-supplied program. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. Therefore, employees should use caution when installing new software on their mobile devices and be vigilant of malicious intent.

## Illegal Activities

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, international, or other applicable laws. Such actions may include, but are not limited to, the following:

* Unauthorized Port Scanning
* Unauthorized Network Hacking
* Unauthorized Packet Sniffing
* Unauthorized Packet Spoofing
* Unauthorized Denial of Service
* Unauthorized Wireless Hacking
* Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
* Acts of Terrorism
* Identity Theft
* Spying
* Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material
* Downloading, storing, or distributing copyrighted material

The company will take all necessary steps to report and prosecute any violations of this policy.

## Reporting of Incident

All Acceptable Use violations will be recorded and investigated on a case by case basis. The following workflow depicts how all AUP incidents will be escalated, investigated, and remediated:

## Applicability of Other Policies

This document is part of the company’s cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

## Audits

The company must conduct periodic reviews to ensure policy compliance. A sampling of users must be taken and audited against this policy on a yearly basis.

# Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

# Revision History

Revision 1.0, 6/19/2012

## 

© 2012 Websense, Inc. All rights reserved. Websense and the Websense logo are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the property of their respective owners.