

# Websense® Mobile Acceptable Use Policy Kit

## **Physical Security Requirements**

### 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. |

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

# Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is increasing. Special consideration must be given to the security of mobile devices.

# Purpose

This policy applies to company data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with company data.

# Scope

This policy applies to employees as it relates to their ability to bring personal mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, tablets, PDAs, smart phones, and USB drives on to the corporate network.

 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.

# Policy

## Physical Security

Employees should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

* Mobile devices should be kept out of sight when not in use.
* Mobile devices should be password protected in accordance with IT security policies.
* Care should be given when transporting mobile devices in busy areas.
* As a general rule, mobile devices must not be stored in cars.  If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment, such as a glove box.

## Laptops

## Whole disk encryption is to be enforced, if available. Laptops must require a username and password or biometrics for login.

## PDAs, Smart Phones, Mobile Devices

Encryption, if available, and login passwords are required on PDAs/smart phones.

## Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of company data on such devices is discouraged, but their use is permitted and encryption should be enforced if available, but is not required.

## Portable Media Players

## No company data can be stored on personal media players.

## Other Mobile Devices

Unless specifically addressed by this policy, storing company data on other mobile devices, or connecting such devices to company systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

## General Guidelines

The following guidelines apply to the use of mobile devices:

* Loss, theft, or other security incident related to a company-provided mobile device must be reported within 24 hours and be accompanied with an official police report. Please refer to the [Security Incident Report](#SIR).
* Confidential data should not be stored on mobile devices, unless it is absolutely necessary.  If confidential data is stored on a mobile device it must be appropriately secured.
* Data stored on mobile devices must be securely disposed of in accordance with the Record Retention Policy.
* Users should take care when storing company data on non-company-provided mobile equipment.  Effort should be taken to minimize the storage of company data. This applies to email, attachments, and local storage of attachments and information. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.
* All data on the device can and will be deleted remotely. This is done to prevent data leakage when the device is lost, stolen, compromised, or when an employee is no longer employed.

## Audits

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

## 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.

# 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.