Mobile Employee Endpoint Responsibility Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the policy for your organization*

Last Update Status: *Retired*

1. Overview

See Purpose.

2. Purpose

This document describes Information Security's requirements for employees of <Company Name> that work outside of an office setting.

3. Scope

This policy applies to any mobile device, or endpoint computer issued by <Company Name> or used for <Company Name> business which contains stored data owned by <Company Name>.

4. Policy

All employees shall assist in protecting devices issued by <Company Name> or storing <Company Name> data. Mobile devices are defined to include desktop systems in a telework environment, laptops, PDAs, and cell phones.

Users are expressly forbidden from storing <Company Name> data on devices that are not issued by <Company Name>, such as storing <Company Name> email on a personal cell phone or PDA.

4.1 Anti-Virus, Secunia CSI and Endpoint Security Software
<Company Name> will issue computers with Secunia, Anti-virus and Endpoint security installed. Employees are to notify the security department immediately if they see error messages for these products. Employees shall run on online malware scanner at least once a month for a "second opinion", see *MS Endpoint Privacy & Security Guidelines* for recommended scanners.

4.2 Browser Add-ons
In general, <Company Name> does not recommend using Browser Add-ons, however we do not forbid the use of these tools if they enhance productivity. After installing a Browser Add-on, employees shall run a browser testing tool. See *MS Endpoint Privacy & Security Guidelines* for recommended testing tools.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

- MS Endpoint Privacy & Security Guidelines

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
Oct 2008	SANS Policy Team	Initial Version
July 2014	SANS Policy Team	Converted to new format and retired. Appropriate items merged into Trusted Device Policy.