Mobile Employee Endpoint Responsibility Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

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

2.0 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>.

3.0 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.

3.1 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 <Company Name> Microsoft Security and Privacy Manual for approved scanners.

3.2 Browser Addons
In general, <Company Name> does not recommend using Browser Addons, however we do not forbid the use of these tools if they enhance productivity. After installing a Browser Addon, employees shall run a browser testing tool. See <Company Name> Microsoft Security and Privacy Manual for testing tools.

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

5.0 Revision History
1.0 initial policy version, 10/29/2008