IT Asset Management Policy

<DATE>
<OFFICIAL SPONSORING POLICY> i.e. Director of Information Technology, John Doe
ISO/IEC 27001 A.7.1.1

Purpose

The purpose of the IT Asset Management Policy is to maintain accurate records of the firm's physical computer assets. This document establishes procedures to ensure compliance with government regulations, legal industry standards and to ensure accurate reporting of physical assets.

Scope

This policy will apply to all computer equipment and related assets purchased by <firm>

Safeguarding Responsibilities

All items purchased will be recorded and maintained on a Fixed Asset Register by the IT Department. In order to manage the register accurately and efficiently, all employees shall adhere to the following;

1) Employees of <firm> shall not remove IT assets supplied by the firm from company premises, except under the following conditions:
    a. IT assets assigned to employees, which may include laptop or tablet computers and Personal Digital Assistant (PDA) or Smartphone devices, may be removed from for the following reasons only:
        1. Teleworking.
        2. Work that is outside of the office that is a part of an assigned position.

    b. Exceptions to this policy must be requested in writing and approved by the Director of Information Security. Documentation of exceptions shall include the business or technical justification and the duration of the exception.

2) Firm employees are responsible for safeguarding any IT assets they remove from the building, including keeping these assets under their direct physical control whenever possible, and physically securing the assets when they are not under the employee's direct physical control.

3) Firm employees must immediately report the loss or theft of any assigned IT assets to the IT Department.

4) Firm employees are not allowed to bring their own IT assets into work locations with the purpose of connecting to the firm's private network and data.
    a. In general, connection of personal IT assets to networks provided by the firm for guest or public access is not allowed.
    b. Exceptions to this policy must be documented in writing and approved by the Director of Information Security. Documentation of exceptions shall include the business or technical justification and the duration of the exception.

Disposal of Assets

Disposal of firm assets, including the sale, transfer, donation, write off or sustainable disposal (recycling), must be done in adherence with all federal, state and local regulations. Computer hardware must have all software and information securely removed prior to disposal.

Highly sensitive data must be deleted using secure methods as soon as they are no longer required. Secure methods of removal shall mean the use of software the can be configured to overwrite the data at least three times and or physical destruction of the hard drives to the extent that precludes any possible restoration of the data.