**Use and Monitoring of Company Property Policy**

**Purpose**

The purpose of this policy is to ensure that all property maintained by [Company Name] is kept in the best possible working condition and to ensure proper use of such property and [Company Name] networks.

“Property,” as the term is used in this policy, is defined as any piece of equipment, furnishing, vehicle, building or supply leased, owned, donated or otherwise in the custodial care of [Company Name] or any person acting as its agent.

No [Company Name] employee should expect any privacy on [Company Name] premises or when using [Company Name] property or networks, except that which is required by law.

**General Guidelines on the Use of Company Property**

All [Company Name] employees must maintain their work environment in an orderly fashion and follow all [Company Name] rules to ensure its proper use and maintenance.

Any employee who is found to have neglected or misused [Company Name] property will be subject to disciplinary action up to and including termination. If an employee’s misuse of [Company Name] property damages the property, [Company Name] reserves the right to require the employee to pay all or part of the cost to repair or replace the property. Misappropriation of [Company Name] property is grounds for immediate termination and possible criminal action.

No employee may use [Company Name] property (including but not limited to computers, telephones, cellphones, copiers, faxes, Internet services and printers) for personal use unless specific permission has been granted by the employee’s department head. If such permission is granted, the employee will be responsible for the care and return of the loaned property. Special care should be taken to identify any concerns regarding its condition before the property is removed or used by the employee for personal use.

**Use of Company Vehicles**

Any employee for whom driving is an essential job duty must be authorized and approved by [department name] to drive [Company Name] vehicles. It is the responsibility of the employee driver of a [Company Name] vehicle to ensure that the vehicle is in full operational condition before each use. The employee driver will sign a vehicle log report noting any problems with, or damage to, the vehicle before each use. Should the employee return the vehicle to the company with damage to the vehicle, the vehicle log report will be used as support evidence of the condition of the vehicle before it was used by the employee driver. Any vehicle found to be unsafe will be removed from the operational fleet until appropriate maintenance or repairs have occurred.

**Use and Dissemination of Company Information**

“Information,” as the term is used in this policy, includes without limitation any information owned or used by [Company Name], such as:

* Any company employee, customer or client lists.
* Any company database information, including addresses and telephone numbers.
* Any information from [Company Name] employee personnel files, including employee addresses, telephone numbers, employment status and wage history.
* Any photographs, videotapes and sound clips of any [Company Name] employee, customer or client.

Only those employees who are authorized by [Company Name]’s board of directors or executive team, or whose job description permits them to do so, may speak on behalf of [Company Name]. Notwithstanding the foregoing, specific permission from the [Company Name]’s board of directors or executive team will be required before any [Company Name] employee may disseminate confidential [Company Name] information.

No employee may knowingly dispense such information to any outside party unless authorization has been granted. This could include other employees who do not have the right to know such information. Any breach will be considered a violation of [Company Name] policy concerning confidentiality, and it may constitute a violation of state or federal law.

**Monitoring of Network Communications**

[Company Name] reserves the right to monitor at any time any communications that use [Company Name] networks in any way, including data, voice mail, email, telephone logs, Internet use and network traffic, to determine proper use.

[Company Name] will review network communications activity and will analyze use patterns. [Company Name] may choose to publish these data to ensure that company resources in these areas are being used according to this policy.

No employee may knowingly disable any network software or system identified as a monitoring tool.