****

**Dial-In Access 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**

The purpose of this policy is to protect <Company Name>'s electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

**2.0 Scope**

The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

**3.0 Policy**

<Company Name> employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication. [Add something in about how “Dial –in access should be requesting using the corporate account request process”]

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to <Company Name> is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and <Company Name> are literal extensions of <Company Name>'s corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect <Company Name>'s assets.

Analog and non-GSM digital cellular phones cannot be used to connect to <Company Name>'s corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to <Company Name>'s network. For additional information on wireless access to the <Company Name> network, consult the *Wireless Communications Policy*.

Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

**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**