Router Security Policy

1.0 Purpose
This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of <*Company Name*>.

2.0 Scope
All routers and switches connected to <*Company Name*> production networks are affected. Routers and switches within internal, secured labs are not affected.

3.0 Policy
Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
2. The `enable secret password` on the router must be kept in a secure encrypted form. The router must have the `enable secret password` set to the current production router password from the Network Operations organization. The `enable password` command should not be used.
3. Routers must comply with the standards outlined in the **Router IOS Template** *(See attachment 1 of this document)* . Routers that do not meet these standards will be re-engineered as needed.
4. Disallow the following:
    a. Incoming packets at the router sourced with invalid addresses such as RFC1918
    b. Incoming packets at the router sourced with <*Company Name*> addresses (spoofing)
    c. TCP and UDP "small services"
    d. All source routing
    e. All web services running on router
    f. IP directed broadcasts
    g. Cisco Discovery Protocol (CDP) on all Third Party interfaces
5. Use corporate standardized SNMP community strings. Community strings "public" and "private" should never be used.
6. Every router should save system logging information to a local RAM buffer in addition to a secured "syslog" server.
7. Any VTY (Virtual Terminal) should be configured to accept connections only with the protocols actually needed. (SSH should be used when possible.) VTY timeouts and a restrictive access-class should be enforced.
8. Each router must have the following statement posted in clear view:

```
NOTICE:  This system is to be used ONLY by AUTHORIZED personnel.

         Any unauthorized use of the system is unlawful, and may
         be subject to civil and/or criminal penalties.

         Use of the system may be logged or monitored without further notice.
```

9. All routers must be included in the corporate enterprise management system (MRTG and Network Node Manager) with a designated point of contact.
10. Security patches and IOS upgrades will be applied as needed during a designated maintenance window. It is the responsibility of the Network Operations organization to keep up-to-date with new security vulnerabilities.

Every switch must meet the following configuration standards:

1. Ports without any need to trunk, should have any trunk settings set to off, as opposed to auto.
2. Trunk ports should use a virtual LAN (VLAN) number not used anywhere else in the switch.
3. Disable any port that is not needed.

4. Disable Spanning Tree Portfast on any port that is attached to a router, firewall or load balancing switch.
5. Hard code speed and duplex settings on all ports, as opposed to auto.
6. Core switches must be assigned a private internal IP address in a “management Vlan.”

4.0 Definitions

Terms	**Definitions**
Production Network	The "production network" is the network used in the 24/7 daily business of <*Company Name*> customers. Any network whose impairment would result in direct loss of functionality to <*Company Name*> customers or impact their ability to do business.
Lab Network	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network and whose impairment will not cause direct loss to <*Company Name*> nor affect the production network.

5.0 Revision History

20011209.1	First Draft	Todd Murchison