Audit Policy

1.0 Purpose

To provide the authority for members of <Company Name>'s InfoSec team to conduct a security audit on any system at <Company Name>.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to <Company Name> security policies
- Monitor user or system activity where appropriate.

2.0 Scope

This policy covers all computer and communication devices owned or operated by <Company Name>. This policy also covers any computer and communications device that are present on <Company Name> premises, but which may not be owned or operated by <Company Name>.

3.0 Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of <Company Name>'s InfoSec team.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on <Company Name> equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on <Company Name> networks.

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