1.0 Purpose

The purpose of this policy is to establish standards for the initial setup and continued configuration management of server equipment that is owned and/or operated by Saint-Gobain Corporation (SGC). Effective implementation of this policy will tighten security for SGC proprietary information and technology assets.

2.0 Scope

This policy applies to server equipment owned and/or operated by SGC, and to servers registered under any SGC owned internal network domain. This policy is specifically for equipment on the internal SGC network. For secure configuration of equipment external to SGC on the DMZ, refer to the Internet DMZ Equipment Policy.

3.0 Policy

3.1 Ownership and Responsibilities:

- All internal servers deployed at SGC must be owned by an operational group that is responsible for system administration. The business group's local IT department must monitor configuration compliance and implement an exception policy (approved by the branch Security Officer) tailored to their environment.

- Servers must be registered with the local Security Officer. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact.
  - Hardware and Operating System/Version.
  - Main functions and applications, if applicable.
3.2 Configuration

- Servers must not be put on the network until up to date antivirus, service packs and security patches have been applied. (The only exception is temporary machine specific configuration purposes).
- Services and applications that will not be used must be disabled.
- Access to services must be logged and/or protected through access-control methods.
- Security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Always use standard security principles of least required access to perform a function.
- Servers must be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled areas, such as cubicles and factory floors.

3.3 Monitoring

All security-related events on critical or sensitive systems must have logging enabled and audit trails saved.

- Suspicious server log events must be reported to the local Security Officer.
- Suspicious events include, but are not limited to:
  - Port-scan attacks.
  - Evidence of unauthorized access to privileged accounts.
  - Anomalous occurrences that are not related to specific applications on the host.

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 Definitions

**DMZ (De-militarized Zone):** A network segment external to the corporate production network.

**Server:** For purposes of this policy, a Server is defined as an internal Saint-Gobain Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.