GRAFIX GARAGE

Security Policy

Security Policy

Purpose

The purpose of this policy is to establish standards for the base configuration of host server equipment that is owned and/or operated by Grafix Garage. Effective implementation of this policy will minimise unauthorised access to Grafix Garage server equipment.

Scope

This policy applies to server equipment owned and/or operated by Grafix Garage, and to servers registered under any Grafix Garage-owned internal network domain. This policy is specifically for equipment used for Grafix Garage web hosting services.

Policy

General Configuration Guidelines

Operating System configuration should be in accordance with approved internal guidelines.

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Security principles of least required access to perform a function is employed where possible.
- Root access will not be used when a non- privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers are physically located in an access-controlled environment.

Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental backups will be retained for at least 1 week.
- Weekly full backups of logs will be retained for at least 1 month.
- Security-related events will be reported to Grafix Garage administration. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific websites on the host.

Compliance

Audits will be performed on a regular basis by authorised organisations within Grafix Garage. Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Server: For purposes of this policy, a Server is defined as a Grafix Garage website hosting Server. Desktop machines are not relevant to the scope of this policy.