Server Security Policy

ChilledWeb Limited

Policy Name:	Server Security Policy	Policy Ref:	CWSSAP
Date of Last Revision:	12 January 2021	Version No:	1.1

Contents

Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by ChilledWeb. Effective implementation of this policy will minimise unauthorised access to ChilledWeb proprietary information and technology.

Scope

All employees, contractors, consultants and temporary workers must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by ChilledWeb or registered under a ChilledWeb-owned internal network domain.

Policy

General Requirements

All servers deployed by ChilledWeb must have a group (team) identified that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the Directors.

The following items must be met:
- Servers must be registered within the corporate enterprise management system. 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
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

For security, compliance and maintenance purposes, authorised personnel may monitor and audit equipment, systems, processes and network traffic.

Configuration Requirements

- Operating System configuration should be in accordance with approved industry 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 a web application firewall, 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 is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root 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 should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled office areas.

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 month.
- Weekly full backups of logs will be retained for at least 1 month.

Security-related events will be reported to the Directors, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
- Port-scan attacks
- Evidence of unauthorised access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host

Exceptions

Any exception to the policy must be approved by the Directors in advance.

Non-Compliance

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