Security Configuration Standard — Web Server Software

1. Purpose

The purpose of this standard is to define the required security configuration settings for all web server software deployed and maintained by **Centerbase**. These configurations are designed to protect systems and data from unauthorized access, reduce vulnerabilities, and ensure consistency across environments.

2. Scope

This standard applies to all web servers used in production, staging, and development environments that host or process company or client data. This includes, but is not limited to, servers running **Microsoft IIS**, **NGINX**, or **Apache HTTP Server**.

3. Configuration Requirements

a. Baseline Hardening

- Apply the latest **vendor security patches** and updates prior to deployment.
- Disable or remove all **unused modules, services, and sample applications**.
- Change or disable **default accounts and passwords**.
- Restrict file and directory permissions to least privilege.

b. Network and Access Controls

- Limit administrative access to authorized personnel only.
- Require **multi-factor authentication (MFA)** for administrative interfaces.
- Place web servers behind a **firewall** or **Web Application Firewall (WAF)**.

c. Encryption and Communication Security

- Enforce **TLS 1.2 or higher** for all communications.
- Disable insecure protocols (e.g., SSLv2, SSLv3, TLS 1.0, TLS 1.1).

- Use strong ciphers as recommended by current **CIS Benchmarks**.

d. Logging and Monitoring

- Enable detailed **access and error logging**.
- Forward logs to a **centralized log management system** for review and retention.
- Monitor for and alert on anomalous or unauthorized activity.

e. Security Headers and Application Settings

- Implement **secure HTTP headers** (e.g., Content-Security-Policy, X-Frame-Options, X-XSS-Protection).
- Disable directory browsing and directory listing.
- Use **least privilege** for any application service accounts.

f. Periodic Review

- Configurations are reviewed **annually or upon major updates**.
- Compliance is validated through **automated scans and manual reviews**.