# TLS Verification Sample Document

## Document Title: TLS Verification Procedure

### 1. Introduction

This document outlines the steps required to verify the TLS configuration for our servers.

### 2. Purpose

To ensure the security of communications by validating the TLS certificates and settings.

### 3. Scope

This procedure applies to all web servers using TLS for secure communications.

### 4. Prerequisites

- Access to the web server
- OpenSSL installed on the local machine
- Administrative permissions

### 5. Verification Steps

#### 5.1 Check TLS version

1. Open a terminal.
2. Execute the following command:
 ```
 openssl s_client -connect <hostname>:443 -tls1_2
 ```
3. Verify the output for TLS version 1.2 or higher.

#### 5.2 Verify the SSL certificate

1. Run the command:
 ```
 echo | openssl s_client -connect <hostname>:443
 ```
2. Review the certificate details:
 - Validity period
 - Issuer
 - Subject

#### 5.3 Check for Intermediate Certificates

1. Use the command:
 ```
 openssl s_client -connect <hostname>:443 -showcerts
 ```
2. Ensure all necessary intermediate certificates are presented.

#### 5.4 Validate Cipher Suites

1. Test available cipher suites using:
 ```
 openssl s_client -connect <hostname>:443 -cipher <cipher_suite>
 ```
2. Ensure only strong ciphers are used.

### 6. Documentation

Record all findings in the TLS Verification Report template.

### 7. Conclusion

Complete the TLS verification and address any issues identified in the report.

### 8. Appendix

- TLS Verification Report Template
- Links to additional resources for TLS configuration best practices.

---

**TLS Verification Report Template**

| Field | Description |
|---------------------|-----------------------------------|
| Date | [Insert date] |
| Server Hostname | [Insert hostname] |
| TLS Version | [Insert version] |
| Certificate Validity | [Valid/Invalid] |
| Intermediate Certs | [Present/Absent] |
| Cipher Suites | [List used cipher suites] |
| Comments | [Any additional notes] |

---

**End of Document**