## [HOST HARDENING PROCEDURE]

*[This is an example for one system]*

Step-by-step documentation of the host hardening of [Server Name]

**Server Access**

[Document the team or personnel with access to the server; Document the roles and access rights available and how access is restricted]

**External Connection Monitoring**

[Document how the external connection is restricted, such as firewall configurations, VPN, IDS, IPS, Whitelisting, other authorization rules]

**Patching Vulnerabilities**

[Document how the server is patched, and plugins are updated]

**Utilities Programs**

[Document how unnecessary software or utilities are reduced on the server. Document whether a tool is in place to manage such utilities and remove unnecessary components ]

**Monitoring**

[Document the type of monitoring of the server in place for suspicious activity]

**Communications**

[Document the type of data encryption Protocols & Cipher Suites for the Communications]

**Credentials protection**

[Document if any, the additional security measures on the server such as anti-virus/anti-malware, strong password, key rotations, access review, auto/lock OS features]

**Backup Plans**

[Document the type of data backup in place]

**Inactive sessions**

[Document how you keep server clock in-sync and lock out sessions after period of time]

**Harden Remote Sessions**

[Document if remote sessions are in place for the server and how one would access it]

**Use Recommended Security Configurations**

[Document if any security standard/best practice was used in configuring the server and link to the standard. For example: [Windows Security Baseline](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines)