**Cybersecurity Templates**

**Server Upkeep & Maintenance Policy & Checklist**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Server Upkeep & Maintenance Policy & Checklist** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy ID:** |  | **Owner:** |  |
| **Effective Date:** |  | **Review Cycle:** |  |

Contents

[Server Upkeep & Maintenance Policy & Checklist 4](#_Toc207131176)

[1. Purpose 4](#_Toc207131177)

[2. Scope & Applicability 4](#_Toc207131178)

[3. References & Related Standards 4](#_Toc207131179)

[4. Definitions (selected) 4](#_Toc207131180)

[5. Roles & Responsibilities 4](#_Toc207131181)

[6. Maintenance Governance 5](#_Toc207131182)

[7. Cadence of Server Upkeep 5](#_Toc207131183)

[7.1 Daily / Per‑Shift (Operations Hygiene) 5](#_Toc207131184)

[7.2 Weekly 6](#_Toc207131185)

[7.3 Monthly 6](#_Toc207131186)

[7.4 Quarterly 6](#_Toc207131187)

[7.5 Semi-Annual 6](#_Toc207131188)

[7.6 Annual 6](#_Toc207131189)

[8. Standard Maintenance SOP (Pre‑, Execute, Post‑) 7](#_Toc207131190)

[8.1 Pre‑Maintenance (T‑24h to T‑0) 7](#_Toc207131191)

[8.2 Execute (T+0) 7](#_Toc207131192)

[8.3 Post‑Maintenance (T+0 to T+1h) 7](#_Toc207131193)

[9. Patch & Vulnerability Management 7](#_Toc207131194)

[Severity SLAs: 7](#_Toc207131195)

[10. Backup & Recovery 8](#_Toc207131196)

[11. Logging, Monitoring & Alerting 8](#_Toc207131197)

[12. Access Management 8](#_Toc207131198)

[13. Configuration Management & Baselines 9](#_Toc207131199)

[14. Certificate & Key Management 9](#_Toc207131200)

[15. Platform‑Specific Procedures 9](#_Toc207131201)

[15.1 Windows Server 9](#_Toc207131202)

[15.2 Linux Server 9](#_Toc207131203)

[15.3 Database Servers (SQL Server, PostgreSQL, MySQL) 9](#_Toc207131204)

[15.4 Virtualization (VMware/Hyper‑V/ V/Proxmox) 10](#_Toc207131205)

[15.5 Containers & Kubernetes 10](#_Toc207131206)

[15.6 Cloud IaaS (AWS/Azure/GCP) 10](#_Toc207131207)

[16. Security Agents & Hardening 10](#_Toc207131208)

[17. Capacity & Housekeeping 10](#_Toc207131209)

[18. Network & Firewall Hygiene 11](#_Toc207131210)

[19. Post‑Maintenance Validation & Acceptance 11](#_Toc207131211)

[20. Exceptions & Risk Acceptance 11](#_Toc207131212)

[21. Documentation & Evidence 11](#_Toc207131213)

[22. Audit & Control Mapping (informative) 11](#_Toc207131214)

[23. Training & Awareness 11](#_Toc207131215)

[24. Incident Handling During Maintenance 12](#_Toc207131216)

[25. Version Control 12](#_Toc207131217)

[Appendices (Forms & Working Templates) 12](#_Toc207131218)

[Appendix A — Maintenance Window Runbook (Fill‑In Form) 12](#_Toc207131219)

[Appendix B — Post‑Change Acceptance (CAT) Checklist 12](#_Toc207131220)

[Appendix C — Server Build Baseline Checklist 13](#_Toc207131221)

[Appendix D — EDR/AV Exclusions Register (Controlled) 13](#_Toc207131222)

[Appendix F — DR/Restore Test Report 13](#_Toc207131223)

[Appendix G — Exception Register 13](#_Toc207131224)

# Server Upkeep & Maintenance Policy & Checklist

# 1. Purpose

This document outlines the standards, cadence, and evidence necessary to maintain servers' security, reliability, and audibility. It unifies routine upkeep (patching, backups, monitoring), change governance, and platform-specific procedures into a repeatable operating model.

# 2. Scope & Applicability

* **In scope:** Windows and Linux servers; hypervisors; container/Kubernetes nodes; database servers (SQL Server, PostgreSQL, MySQL); application servers; domain services (AD/LDAP/DNS/NTP); cloud compute (AWS/Azure/GCP); bastion/jump hosts.
* **Out of scope:** End‑user devices, network appliances (covered by the Network Upkeep Policy), SaaS platforms managed by vendors (see the Vendor Security SOP).
* **Priority:** Production > pre‑prod > test/dev. Tasks are applied proportionally based on criticality and data sensitivity.

# 3. References & Related Standards

* Information Classification & Handling Standard
* Vulnerability & Patch Management Standard
* Identity & Access Management (IAM) Standard
* Incident Response Plan and Disaster Recovery Plan
* Secure Configuration Baselines (e.g., CIS Benchmarks)

# 4. Definitions (selected)

* **CAB:** Change Advisory Board that approves changes and maintenance windows.
* **CAT:** Customer/Change Acceptance Testing following maintenance.
* **EDR:** Endpoint Detection & Response agent.
* **RPO/RTO:** Recovery Point Objective / Recovery Time Objective.
* **Snapshot:** Point-in-time VM/volume copy used for rollback.

# 5. Roles & Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Evidence/Deliverables** |
| Service Owner | Defines SLOs, approves maintenance windows, and signs post-change acceptance. | Signed window approval; CAT sign‑off |
| System Administrator | Executes tasks, captures artifacts, and performs rollback if required. | Change ticket notes; screenshots/logs |
| Security Engineer | Confirms patch/vuln status, EDR health, SIEM logging, cert hygiene. | Vuln report; EDR console status; log ingestion proof |
| DBA | DB backups/integrity, index/stats, version supportability. | Restore test logs; DB integrity report. |
| Network Engineer | Firewall/Security Groups, load balancer, and DNS updates. | Rule diff; DNS/healthcheck proofs |
| Change Manager/CAB | Risk assessment, approvals, communications. | Approved CR; stakeholder comms |

# 6. Maintenance Governance

**Approvals:** All production maintenance requires a CAB‑approved change record with defined scope, risk, rollback plan, and acceptance criteria.  
**Windows:** Standard windows are [weekday/timezone] after-hours. Emergency windows are allowed for Critical vulnerabilities/outages with post‑facto CAB review.  
**Staging:** All changes follow **Dev → Test → Pre‑Prod → Prod** progression, with evidence at each stage.  
**Freeze Periods:** Defined seasons (e.g., quarter‑end) where only emergency changes proceed.  
**Communications:** Stakeholders notified **T‑5 days** (standard) or **as‑soon‑as‑practicable** (emergency)—templates provided in Appendix A

# 7. Cadence of Server Upkeep

Each cadence has **Tasks**, **Acceptance Criteria**, and **Evidence**. Record outcomes in the maintenance ticket and attach artifacts.

## 7.1 Daily / Per‑Shift (Operations Hygiene)

* **Tasks:** Confirm backups completed; check critical/failed alerts; verify EDR/AV is healthy and updated; confirm logs are streaming to SIEM; spot‑check disk capacity and key services.
* **Acceptance:** No Critical alerts unacknowledged > 4 hours; backup jobs green; SIEM shows last 2 hours of logs; EDR shows “healthy” posture.
* **Evidence:** NOC dashboard screenshot; backup console status; SIEM query export.

## 7.2 Weekly

* **Tasks:** Apply non-disruptive patches (where hot‑patch or service restart is acceptable); review vulnerability findings; check certificate expiries (<60 days); validate replication jobs; rotate service credentials/tokens per policy.
* **Acceptance:** Zero High vulns older than policy SLA; no certs under 30 days without an active renewal ticket; replications green.
* **Evidence:** Vulnerability report extract; certificate inventory; replication job logs.

## 7.3 Monthly

* **Tasks:** OS and firmware patching per policy; planned reboots; test restore from backup; review admin groups and privileged access; update CMDB.
* **Acceptance:** 95% of servers on current patch baseline; successful restore test for representative workload; admin groups reviewed with sign‑off.
* **Evidence:** Patch compliance report; restore runbook with checksums; IAM access review export; CMDB delta report.

## 7.4 Quarterly

* **Tasks:** DR exercise or targeted restore; firewall/Security Group review; EDR exclusions review; capacity trend analysis; config drift check against baselines.
* **Acceptance:** RPO/RTO validated; stale rules removed; exclusions justified; capacity headroom ≥ 20%; drift remediated or accepted.
* **Evidence:** DR report; firewall diff; EDR exclusions register; capacity charts; baseline comparison results.

## 7.5 Semi-Annual

* **Tasks:** Version/supportability review (OS/DB/Hypervisor/K8s); maintenance window effectiveness review; privileged access audit; runbook refresh.
* **Acceptance:** No unsupported versions in production; documented improvements to window length/comms; privileged access attested.
* **Evidence:** Support matrix; audit attestations; updated runbooks.

## 7.6 Annual

* **Tasks:** Full failover (where feasible); key/certificate rotation for long-lived assets; tabletop incident drill; policy review and attestation.
* **Acceptance:** Pass/fail documented with actions; rotation logs; lessons learned tracked to closure.
* **Evidence:** Failover report; PKI rotation log; tabletop minutes; signed policy review.

# 8. Standard Maintenance SOP (Pre‑, Execute, Post‑)

## 8.1 Pre‑Maintenance (T‑24h to T‑0)

1. **Verify backups & test restore:** Confirm last successful backup; perform **targeted restore test** (file/DB) in non-prod; record checksums and screenshots.
2. **Create rollback points:** VM/volume snapshots for all impacted systems with retention of ≥ 72 hours.
3. **Health baseline:** Capture CPU/memory/disk, service status, application synthetic checks, and latency to dependencies.
4. **Access & console:** Verify privileged access, break‑glass credentials sealed, and out-of-band console reachable.
5. **Monitoring:** Place noisy alerts in maintenance mode while retaining critical health alarms.
6. **Communications:** Send start reminder with impact, contact, and timeline; update status page if applicable.

## 8.2 Execute (T+0)

1. Follow the change steps in order; log each step with timestamps.
2. Apply patches/updates; reboot in maintenance waves if clustered.
3. Validate security agents remain healthy (EDR/AV, file integrity, logging).
4. If failure thresholds are met, **initiate rollback** immediately and escalate.

## 8.3 Post‑Maintenance (T+0 to T+1h)

1. **Functional checks:** Smoke tests (login, core transactions, API endpoints).
2. **Dependency checks:** DB connectivity, message queues, file shares, DNS, TLS endpoints.
3. **Monitoring:** Re-enable alerts; ensure no new Critical alarms for ≥ 30 minutes.
4. **Evidence:** Attach logs, screenshots, versions, and health reports to the ticket.
5. **Comms:** Send completion notice with residual risks and next steps.

# 9. Patch & Vulnerability Management

## Severity SLAs:

| **Severity** | **Example** | **Remediation Target** |
| --- | --- | --- |
| Critical (exploited/remote code) | High-impact kernel/SSL/AD flaws | ≤ 7 days |
| High | Privilege escalation, auth bypass | ≤ 14 days |
| Medium | Misconfigurations, non-network RCE | ≤ 30 days |
| Low | Informational | As scheduled |

* **Patch Rings:** 1) Canary (non‑prod) → 2) Low‑risk prod → 3) General prod → 4) Regulated/mission‑critical.
* **Deferral:** Allowed only with documented **risk acceptance** and compensating controls (e.g., WAF rules, service isolation).
* **Emergency Patching:** Changes may proceed outside the window if risk dictates; a post-implementation review with the CAB is required within 48 hours.

# 10. Backup & Recovery

* **Types:** Image‑level, file‑level, and application‑aware (e.g., VSS, RMAN).
* **Schedules:** Daily incrementals; weekly fulls; transaction/log backups as applicable.
* **Retention:** Production ≥ 30 days (or per regulatory needs); offsite copy maintained; backups **encrypted** in transit and at rest.
* **Restore Tests:** At least monthly per service class; record RTO/RPO achievement and issues.
* **DR:** Replication health monitored; quarterly failover or targeted recovery test.

# 11. Logging, Monitoring & Alerting

* **Centralization:** System, security, and application logs forward to SIEM; time synchronized via NTP/AD.
* **Coverage:** EDR telemetry, OS audit logs, auth events, web/app logs, and infrastructure metrics.
* **Retention:** Per legal/regulatory requirement; tamper-evident storage for security logs.
* **Health:** Alerts for agent outages, log pipeline failures, and clock skew.

# 12. Access Management

* **Principle:** Least privilege; role-based access with periodic reviews.
* **Admin Access:** MFA enforced; no shared local admin; break‑glass accounts in sealed vault with rotation and alerts on use.
* **Service Accounts:** Password/secret rotation; key material stored in approved vault; usage logged.

# 13. Configuration Management & Baselines

* **Baselines:** Apply and track secure baselines (e.g., CIS) per OS/workload.
* **Drift:** Automated detection and remediation; variances must have approved exceptions.
* **Inventory/CMDB:** Accurate server inventory, owners, criticality, environment tags, and dependency mapping.

# 14. Certificate & Key Management

* **Inventory:** Maintain certificate catalog with owners and expiry dates.
* **Renewal:** Alert at 60/30/15 days; automate renewal where possible; enforce modern TLS ciphers/protocols.
* **Key Security:** Protect private keys via HSM or secrets vault; rotate long-lived keys annually or per policy.

# 15. Platform‑Specific Procedures

## 15.1 Windows Server

* Apply approved Windows Updates via WSUS/SCCM/Intune; reboot as required.
* Review Event Viewer (System/Application/Security) for recurring errors and audit failures.
* Validate IIS/.NET apps start cleanly; recycle app pools as needed.
* Confirm Defender/AV signatures and scheduled scans; verify VSS/Shadow Copy health.
* Harden RDP (NLA, restricted groups, MFA via gateway); enforce host firewall.

## 15.2 Linux Server

* Apply apt/yum/dnf updates; plan kernel reboots.
* SSH hardening: Protocol 2, strong ciphers, disable root login, key-based auth; fail2ban or equivalent.
* Review journalctl/syslog; rotate/compress oversized logs; validate iptables/nftables/firewalld rules.
* Enforce SELinux/AppArmor according to baseline; verify NTP/chrony sync.

## 15.3 Database Servers (SQL Server, PostgreSQL, MySQL)

* **Backups:** Full/Diff/Log as applicable; document last successful **restore test**.
* **Integrity:** DBCC CHECKDB (SQL) or equivalent; VACUUM/ANALYZE for Postgres; optimize/repair as approved.
* **Maintenance:** Index rebuild/reorg and statistics updates; partition maintenance.
* **Security:** Least‑privileged roles; TLS enforced; credential rotation and secret storage in a vault.
* **Supportability:** Engine version supported; compatibility levels reviewed quarterly.

## 15.4 Virtualization (VMware/Hyper‑V/ V/Proxmox)

* Cluster health (HA/DRS/Live Migration) green; datastore usage <80%.
* ESXi/host OS patch level supported; tools/agents updated on VMs.
* Remove or justify snapshots older than policy threshold.
* Validate vSwitch/port group security settings and DVS consistency.

## 15.5 Containers & Kubernetes

* Cluster and node versions supported; apply security patches and address CVEs.
* etcd backup tested; control plane cert/key rotation per policy.
* Admission controls and network policies enforced; image scanning passing; restrict privileged pods.
* Resource quotas and requests set; audit/OPA policies applied.

## 15.6 Cloud IaaS (AWS/Azure/GCP)

* **IAM:** Least privilege; periodic access reviews; API keys older than policy rotated.
* **Networking:** Security Groups/NSGs reviewed; unused rules removed; flow logs enabled.
* **Backups/Snapshots:** Schedules and retention verified; cross‑region copies healthy; lifecycle policies enforced.
* **Monitoring:** Metrics/alarms configured (CPU, memory where available, disk, status checks); logs centralized; cost/quotas monitored.

# 16. Security Agents & Hardening

* **EDR/AV:** Installed and “healthy” on all servers; exclusions minimized and reviewed quarterly.
* **File Integrity Monitoring:** Enabled for critical paths; alerts triaged.
* **Hardening:** Disable unused services; enforce least functionality; validate boot security and disk encryption where supported.

# 17. Capacity & Housekeeping

* Maintain disk usage <80% or document exception with cleanup plan.
* Prune temporary and log directories per retention; rotate and compress large logs.
* Track CPU/memory trends; scale before saturation; document capacity decisions.

# 18. Network & Firewall Hygiene

* Host firewalls enabled with default‑deny where feasible; only required ports open.
* Validate DNS resolution, NTP, and time skew; check baseline latency to dependencies.
* Review inbound/outbound allow‑lists quarterly; document changes.

# 19. Post‑Maintenance Validation & Acceptance

* **Smoke Tests:** Documented outcomes for key user flows and API health.
* **Regression Checks:** Compare performance to baseline; investigate deltas.
* **Monitoring:** Ensure alerting is restored and stable for ≥ 30 minutes.
* **Sign‑Off:** Service Owner or delegate signs CAT; CAB records closure.

# 20. Exceptions & Risk Acceptance

* Exceptions must detail scope, risk, compensating controls, owner, and expiry (≤ 90 days unless extended).
* Maintain an **Exception Register** (Appendix G) with review cadence and closure actions.

# 21. Documentation & Evidence

* Attach artifacts to the change ticket: patch reports, backup/restore logs, screenshots, configuration diffs, SIEM queries, EDR health, certificate lists.
* Retain evidence per Records Retention Policy.

# 22. Audit & Control Mapping (informative)

This procedure supports controls in areas such as operational security, change management, backup & recovery, logging/monitoring, and vulnerability management. Control owners should map this template to the relevant framework(s) as needed.

# 23. Training & Awareness

* New administrators complete **Server Upkeep SOP training** before elevated access.
* Annual refresher includes DR tabletop and maintenance simulation.

# 24. Incident Handling During Maintenance

* If maintenance causes a service impact beyond the approved window or acceptance criteria fail, declare a **change incident**, execute rollback, notify stakeholders, and open a problem record for root‑cause analysis.

# 25. Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summary of Change** |
| 1.1 | [YYYY‑MM‑DD] | [Name] | Initial full template release |

# Appendices (Forms & Working Templates)

## Appendix A — Maintenance Window Runbook (Fill‑In Form)

**Change ID:** ………  
**Systems Affected:** ………  
**Owner/Engineer:** ………  
**Start/End (TZ):** ………  
**Impact Summary:** ………  
**Pre‑Checks:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Backups verified ☐ | Test restore completed ☐ | Snapshots created ☐ | Baseline captured ☐ | Access verified ☐ |

**Step‑by‑Step Tasks:** 1) … 2) … 3) … 4) …  
**Rollback Triggers:** …  
**Rollback Steps:** …  
**Comms Plan:**

|  |  |  |
| --- | --- | --- |
| Audience … | Channels … | Cadence: Start ☐ Midpoint ☐ Complete ☐ Incident ☐ |

## Appendix B — Post‑Change Acceptance (CAT) Checklist

* Functional tests: login ☐, transactions ☐, API ☐, batch jobs ☐
* Dependency tests: DB ☐, MQ ☐, fileshares ☐, DNS ☐, TLS ☐
* Monitoring re‑enabled ☐; no Critical alarms for ≥ 30 min ☐
* Performance within ±10% of baseline ☐
* Evidence attached (logs/screenshots) ☐
* **Service Owner Sign‑Off:** Name/Date ………

## Appendix C — Server Build Baseline Checklist

* OS version (supported) ☐
* Secure baseline applied (ID: …) ☐
* EDR/AV installed & healthy ☐
* Time sync configured ☐
* Host firewall rules applied ☐
* Local admin groups reviewed ☐
* Backup agent installed & job assigned ☐
* Monitoring agent installed ☐
* SIEM logging verified ☐
* Certificate store reviewed ☐
* Console/serial access tested ☐

## Appendix D — EDR/AV Exclusions Register (Controlled)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System** | **Path/Process** | **Justification** | **Approval (Security)** | **Review Date** |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

**Appendix E — Certificate Inventory**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Service** | **FQDN** | **Owner** | **Expiry Date** | **Status** | **Renewal Ticket** |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Appendix F — DR/Restore Test Report

**Service:** ………  
**Scenario:** Targeted restore ☐ | Full failover ☐  
**RPO Achieved:** …  
**RTO Achieved:** …  
**Issues/Actions:** …  
**Owner/Date:** …

## Appendix G — Exception Register

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Scope** | **Risk** | **Compensating Controls** | **Owner** | **Expiry** | **Status** |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |