Duties/Responsibilities-Possible Standard Operating Procedures and Possible Optimization

1. Maintain the Information Systems infrastructure to support the various users of the company

Standard Operating Procedure:

- Perform daily usage monitoring and resource check of servers using Kaseya, SNMP tools
- Ensure security patches up-to-date through Sophos Endpoint Central
- Check backups completed overnight using Veeam without errors
- Review connectivity monitoring dashboards on SolarWinds (uptime, traffic flow, latency)
- Generate server performance reports weekly using SQL Server Reporting Services for capacity review

Optimization: Create service ticket workflow in ServiceNow to assign, track and report on infrastructure support tasks. Build dashboard for key system health indicators. Automate weekly/monthly report delivery to IT team using Schedule Export in SQL Server Reporting Services.

2. Plan, maintain, and monitor network capacities and capabilities.

SOP:

- Review network performance data, capacity utilization to forecast needed changes
- Perform due-diligence on new networking gear (POC test runs)
- Develop implement plans to phase equipment in during maintenance window
- Update inventory databases and monitoring tools with equipment details
- Test redundancies and failover in staging environment first before deploy

Optimization: Use reporting capabilities in SolarWinds to trigger alerts and tickets for over 80% network capacity. Integrate network configuration management data into ServiceNow CMDB utilizing APIs for unified source of truth.

3. Evaluate, implement, monitor, and maintain various forms of network security

SOP:

- Perform security threat analysis to identify vulnerabilities (servers, firewalls, endpoints)

- Review recommended network segmentation and ACL updates from Cisco Adaptive Security Appliance reports

- Develop phased deployment plan of configuration changes, review with security team

- Implement ACL, firewall policy updates per coordination procedures

- Inform Security Incident Response team if intrusion detection triggered

Optimization: Integrate network access logs with Splunk security analytics system to correlate events and threats with users/devices for enhanced monitoring. Use out-of-band network on Juniper SRX devices for remote security management.

4. Build out and maintain network redundancy and resilience as is practical to meet business needs.

SOP:

- Audit critical infrastructure dependencies and risks

- Architect redundant systems, storage, availability zones to address gaps

- Coordinate upgrades with redundant instances to avoid total outage potential

- Configure redundant systems/instances to failover automatically via cluster manager tools

- Regularly test failover capabilities by performing controlled failovers in lower environments

Optimization: Set up site-to-site connectivity between on-premise and cloud (AWS/Azure) environments to enable real-time replication of critical workloads for cloud DR capabilities.

5. Establish and monitor backups of data to meet business requirements

SOP:

- Classify critical data types for protection levels in collaboration with stakeholders
- Create policies for retention periods for backups stored on secondary NAS devices
- Test end-to-end backup process monthly including artifact validation and system recovery checks
- Investigate failed backup jobs within SLA of next retry attempt
- Generate performance dashboards and reports for backup trends

Optimization: Employ consistent backup configuration templates across similar server/system profiles using Ansible or PowerShell for uniformity and compliance. Use Veeam's Scale-Out Backup Repository capabilities to offload older backup repositories to low-cost capacity storage.

6. Work with contractors, installers, and others to maintain off-site equipment.

SOP:

- Maintain master inventory of all assets at off-site facilities with owner details
- Establish regular maintenance review schedule and coordinate with vendors/contractors
- Issue service requests/purchase orders for work required from external providers
- Review completion of tasks validating assets updated in configuration management database
- Use visitor management procedures that ensure contractors adhere to policies on location

Optimization: Implement tracking tool similar to AssetSonar to log locations and details of assets as they get provisioned on-site or relocated off-site for quicker inventory validation.

7. Look for and investigate anomalous data usage.

SOP:

- Establish data usage baselines for applications, servers, networks
- Perform daily/weekly analysis using security tools to detect deviations
- Review anomalies flagged using automated tools like Darktrace or Splunk
- Research source of anomalies through console logs, system audits
- Inform security team and other admins of potential insider threats

Optimization: Integrate user behavior analytics tools with data loss prevention controls on gateways to better correlate anomalies with users and restrict abnormal data egress.

8. Implement and maintain various tools for monitoring the network.

SOP:

- Document platform requirements for management tools
- Install and configure tools aligning to functional need (security, performance etc)
- Onboard new network segments and key metrics into tools
- Define alerts and thresholds to trigger notifications
- Periodically review efficacy of deployed tools, retire unused

Optimization: Establish centralized dashboard using Grafana consolidating key network health and performance metrics in a single pane of glass. Automate report generation using APIs.

9. Investigate server, database and application performance issues.

SOP:

- Get alerts on degradation from monitoring tools like Datadog
- Review affected application logs to pinpoint failure points
- Identify resources constraints via Perfmon counters and queries
- Reproduce issues in staging to diagnose root cause
- Apply fixes, schedule reboots if necessary and confirm resolution

Optimization: Implement synthetic user monitoring with Catchpoint to simulate production traffic conditions during changes to better validate performance.

10. Maintain the email system and investigate various connectivity, reception, and transmission issues.

SOP:

- Daily review of Office 365 Service Health status
- Check mailbox server queue for deferrals or building delays
- Verify DNS records and TLS certificate validity for mail routing
- Use mail flow tracing and delivery reports to diagnose send/receive issues
- Inform users of maintenance or ISP issues affecting uptime

Optimization: On-premise gateway appliances providing extra email continuity and layered security enabling shadow infrastructure as redundancy to cloud email when needed.

11. Continually work to improve store performance issues.

SOP:

- Set up digital signage boxes powered by Chromebox to display real-time KPIs
- Issue barcode scanners or mobile devices for stock checks and order fulfilment
- Label racks/shelves and map locations in inventory system
- Train staff on how to look up item availability and whereabouts
- Integrate ecommerce platform APIs into ERP/CRM for order visibility

Optimization: Install IoT sensors connected to Sigfox network to automate inventory level tracking and alerts when items need reordering.

12. Work with other departments to reduce costs or improve usefulness by applying experience and knowledge to various issues.

SOP:

- Maintain understanding of other departments' tech needs via liaison meetings
- Identify opportunities to consolidate systems/tools for licensing and ops efficiency
- Provide recommendations balanced to budget constraints
- Handle secure decommissioning of outdated solutions to stop unnecessary costs
- Document implemented solutions in knowledge base for self-service

Optimization: Develop IT roadmap steering committee including leadership across business units to align technology initiatives and investments.

13. Investigate sensitive and confidential issues for Human Resources and executives as needed.

SOP:

- Follow security incident response procedures upon alert from HR
- Isolate and document affected user account details

- Review authentication logs, network access logs to determine exposure

- Check email filters and DLP policies for violations

- Generate audit report with summary of findings

Optimization: Implement privileged access management access reviews and draw down of permissions during employee offboarding.

Let me know if this renumbered format meets your needs or if you need any clarification!