LAS VEGAS-CLARK COUNTY LIBRARY DISTRICT

TECHNOLOGY PLAN FY2026 – 2031

TECHNOLOGY MISSION STATEMENT

The Library District delivers secure, reliable, and innovative technology that empowers staff, enhances customer access, and expands equitable digital services across all branches. Our mission is to modernize our platforms, safeguard our community, and provide intuitive tools that help people learn, work, and create.

EXECUTIVE SUMMARY

This five-year plan modernizes the District's Microsoft 365 environment and core technology operations. It focuses on six priorities that will be delivered through phased programs with measurable outcomes:

- Email modernization: move from on-premises Exchange to a hybrid model with a clear path to cloud-first operations.
- Identity security: enforce multifactor authentication (MFA), enable self-service password reset (SSPR), apply Conditional Access, and eliminate legacy authentication.
- Endpoint standardization: adopt cloud-managed policy baselines in Microsoft Intune and enroll all staff devices for consistent security and updates.
- Threat protection: deploy Microsoft Defender across endpoints, email, collaboration, and identities; operationalize incident response.
- Content modernization: migrate file servers and the Voyager intranet to a modern SharePoint intranet with improved information architecture.
- Long-term governance: advance data protection, least-privilege access, and continuous posture improvement using secure score and Zero Trust practices.

LIBRARY OVERVIEW

The Library District is one of the largest and most complex public library systems in the nation and the largest in Nevada. It serves approximately 1.7 million residents across an 8,000-square-mile area that includes urban and suburban communities throughout the valley, as well as small towns and remote rural regions of Clark County.

The Library District's service area encompasses the City of Las Vegas and most of Clark County, excluding Boulder City, Henderson, and North Las Vegas. With more than 580,000 cardholders, 3.85 million branch visits, 1.33 million computer-use sessions, and over 1.2 million program participants during 2024-2025, the District is among the most active public library systems in the country.

Established in 1965 by the Clark County Board of Commissioners, the District was initially created as a taxing district to provide library services to residents outside the Las Vegas city limits. Originally known as the Greater Clark County Library District, and later the Clark County Library District, it expanded as other taxing districts across the county were consolidated into it. A contract with the City of Las Vegas soon followed, allowing the District to manage libraries within city boundaries. In 1985, legislation enacted by the Nevada State Legislature formalized the system as the Las Vegas-Clark County Library District, the state's first consolidated library district, officially incorporating Las Vegas city libraries into the system.

Today, the Library District operates 25 facilities: 14 located in the urban Las Vegas Valley and 11 serving outlying communities in rural Clark County. Administrative and support functions are based at the Windmill Library and Service Center in the southwest valley.

GUIDING PRINCIPLES

The guiding principles establish a secure, measurable, and scalable foundation for modernizing the Library District's technology environment. They emphasize security by default, cloud-first management, phased delivery, and outcomes-driven decision-making.

- Security by default and Zero Trust: verify explicitly, use least privilege, and assume breach.
- Phased rollouts with pilot rings: validate changes with small cohorts before scaling district-wide.
- Cloud-native management first: standardize configuration in Intune rather than legacy-only approaches.
- Measurable outcomes: use security posture metrics and operational KPIs to prioritize work year-over-year.

Program Governance & Delivery Method

The program is governed through a standardized delivery lifecycle to ensure consistency, accountability, and controlled risk across all workstreams. Clearly defined roles and responsibilities support executive oversight, technical execution, change management, and operational readiness. Each major workstream follows a consistent delivery lifecycle:

- Initiate: kickoff, scope confirmation, success criteria, and timeline.
- Design: current-state assessment and blueprint for configuration/migration.
- Implement: build, configure, test, and document.
- Cutover & Post-Support: execute step-by-step cutover with backout and testing, plus a defined hypercare window.
- Closeout: finalize documentation, knowledge transfer, and operational handoff.

Recommended roles and responsibilities:

- Executive sponsor: sets direction and priority.
- Program owner (IT leadership): manages roadmap and risk decisions.
- Technical leads: Identity/Exchange; Endpoint/Intune; Security/Defender; SharePoint/Intranet.
- Change management lead: communications, training, and adoption.
- Service desk lead: runbooks, escalations, and metrics.

Five-Year Roadmap

The five-year roadmap outlines a phased approach to modernizing identity, security, endpoint management, collaboration, and governance capabilities. Each year builds on the previous one to progressively strengthen security posture, operational maturity, and long-term sustainability.

Year 1 — Foundations: Hybrid Exchange, Identity Security, Intune Baselines, and Staff Device Enrollment

Year 1 outcomes:

- Hybrid Exchange is in place, and mailbox migration is underway using a controlled coexistence approach.
- MFA enforced, SSPR enabled, Conditional Access deployed, and legacy authentication blocked.
- Cloud policy management is established in Intune using security baselines and settings catalog.
- All staff-only computers are enrolled in Intune and receive baseline security, compliance, and update policies.

Year 1 Workstreams & Deliverables

Exchange — On-Premises to Hybrid Exchange and Mailbox Migration Start

Key actions:

- Validate hybrid readiness (versions/CUs, certificates, namespaces, prerequisites).
- Configure hybrid with the Hybrid Configuration Wizard (HCW) to enable coexistence and migration.

- Pilot mailbox moves with IT and a small business cohort; migrate in waves with documented success criteria.
- Align mail flow and DNS to support hybrid coexistence and cloud mail routing.

Deliverables:

- Hybrid Exchange design and namespace/certificate plan.
- Mailbox migration wave plan (pilot → phases → completion criteria).
- Cutover runbook and rollback plan.

Acceptance criteria: Hybrid mail flow functioning, coexistence validated, and pilot mailbox moves completed successfully.

Identity — MFA, SSPR, and Conditional Access

Key actions:

- Deploy Conditional Access policies that require MFA for all users, with emergency access exclusions.
- Block legacy authentication to reduce credential-based attack surface.
- Enable SSPR and use combined registration so users register once for MFA and SSPR.
- Run a registration campaign (communications, quick guides, service desk scripts) to drive enrollment at scale.

Deliverables:

- Conditional Access baseline and staging plan (report-only → pilot → enforced).
- SSPR configuration package and service desk guide.
- Registration communications templates and monitoring approach.

Acceptance criteria: ≥95% of staff enrolled in MFA and SSPR; legacy auth blocked for the general population; support scripts validated.

Endpoint Management — Establish Intune Policy Baselines and Enroll Staff Computers

Key actions:

- Build the Intune tenant foundation: enrollment restrictions, device categories, naming standards, RBAC, and scope tags.
- Define a cloud policy baseline using Settings Catalog, Administrative Templates, and Security baselines.
- Configure Windows update rings for pilot-to-production rollout.
- Create compliance policies for device health and encryption; align to Conditional Access.
- Enroll all staff-only computers in staged waves with remediation runbooks.

Deliverables:

- Intune baseline policy set and configuration catalog.
- Update ring strategy (Pilot → Broad).
- Enrollment migration runbook and troubleshooting flow.
- Compliance reporting and operational dashboards.

Acceptance criteria: ≥90–95% of staff endpoints enrolled and receiving baseline policies; pilot update ring stable; compliance reporting active.

Year 2 — Microsoft Defender Rollout and Security Operations Maturity

Year 2 outcomes:

- Microsoft Defender for Endpoint is deployed and operationalized with risk-based access controls.
- Email and collaboration threat protection is configured to Microsoft-recommended levels (Standard/Strict).
- Identity threat detection is enabled for on-premises identity infrastructure (sensors on domain controllers).
- Cloud app discovery and governance implemented to reduce shadow IT and risky app exposure.
- Security posture improvement is tracked and managed with Secure Score.

Year 2 Workstreams & Deliverables

Defender for Endpoint and Intune Integration

Key actions:

- Establish the Intune Defender connection and onboard endpoints via Intune policies.
- Use Defender device risk in Intune compliance policies and enforce via Conditional Access for noncompliant/high-risk devices.
- Onboard in phases by device group and pilot ring (IT → pilot departments → district-wide).

Deliverables:

- Onboarding policy and validation checklist.
- Risk-based compliance policy and Conditional Access enforcement plan.
- Incident triage workflow (alerts → assignment → remediation → lessons learned).

Defender for Office 365 (Email and Collaboration Protection)

Key actions:

- Implement Microsoft-recommended threat policy settings using preset Standard/Strict levels.
- Configure Safe Attachments protections and validate scope.
- Validate Safe Links behavior aligns to recommended baseline settings.

Deliverables:

- Threat policy baseline (anti-phish, anti-spam, anti-malware, Safe Links, Safe Attachments).
- Tuning and exception process for false positive handling and allow/block governance.

Defender for Identity (Identity Threat Detection)

Key actions:

- Deploy sensors on all domain controllers.
- Use product recommendations to remediate high-risk identity misconfigurations and reduce lateral movement paths.

Deliverables:

- Sensor deployment plan and coverage map.
- Identity posture remediation backlog with timelines.

Defender for Cloud Apps (SaaS Discovery and Governance)

Key actions:

- Enable cloud discovery and risk ranking to identify unsanctioned SaaS usage and risky OAuth apps.
- Implement governance policies for app approval, permission controls, and anomaly detection.

Deliverables:

- Cloud discovery baseline report and quarterly review process.
- Sanction/unsanction policy and governance workflow.

Security Posture Management

Key actions: establish a Secure Score baseline and convert top recommendations into quarterly remediation plans.

Deliverables: quarterly Secure Score improvement plan and executive reporting package.

Year 3 — Migrate File Servers and Voyager Intranet to SharePoint Intranet

Year 3 outcomes:

- File server content migrated into SharePoint and OneDrive using a mapped information architecture and controlled permissions.
- A modern SharePoint intranet (home site, hubs, departmental sites) replaces the Voyager intranet as the primary internal portal.
- Legacy intranet workflows transitioned to Power Automate where applicable.

Year 3 Success Plan

Phase 1 — Discovery & Assessment

- Content inventory (file servers and intranet): identify shares, folder structures, file types, owners, and last-accessed patterns; build a cleanup plan.
- Catalog Voyager intranet pages, navigation, embedded apps, forms, and workflows; prioritize scenarios for modernization.

Phase 2 — Information Architecture & Intranet Design

- Define global navigation, hub structure, and local site navigation.
- Define metadata strategy (content types and columns) to support search and compliance.
- Design intranet structure with a SharePoint home site as the front door and hubs for major functions.
- Standardize page templates and governance for publishing, ownership, and review cycles.

Phase 3 — Build the Target Environment

- Provision SharePoint sites and document libraries; pre-provision OneDrive as needed.
- Implement a permissions model based on groups and clear ownership to reduce operational overhead.
- Prepare migration tooling and ensure prerequisites/endpoints are met.

Phase 4 — Migrate File Servers

- Pilot migrate representative shares with permissions validation and user testing.
- Execute wave migrations by department with a defined freeze window near cutover.
- Validate permissions, file counts, and key business processes; obtain sign-off.

- Cut over mapped drives/shortcuts to SharePoint libraries and Teams where appropriate.
- Decommission or repurpose file servers after acceptance; document exceptions and timelines.

Phase 5 — Migrate Voyager Intranet to SharePoint Intranet

- Define intranet scenarios (news, policies, procedures, forms, IT help, branch operations, employee resources).
- Recreate navigation using the home site, hubs, and modern pages.
- Migrate/replace workflows with Power Automate.
- Improve search and discoverability based on the information architecture and metadata.
- Pilot with one department, iterate, then launch district-wide with training and support.

Acceptance criteria: ≥80% of targeted file server content migrated and validated; intranet home site live with hubs and departmental pages; Voyager intranet moved to read-only with a decommission plan approved.

Year 4 — Data Governance, Compliance, Least Privilege, and Advanced Endpoint Controls

Year 4 outcomes:

- Data protection and classification standard using Microsoft Purview sensitivity labels with policy-based enforcement.
- Privileged access is controlled with just-in-time administration using Privileged Identity Management (PIM).
- Identity governance processes (access reviews and entitlement management) limit access creep.
- Reduced local admin risk through Endpoint Privilege Management (EPM) where appropriate.
- Measured Zero Trust progress with security posture metrics and reviews.

Year 4 Workstreams

Microsoft Purview — Labels and DLP Foundations

- Build and publish a label taxonomy (e.g., Public, Internal, Confidential, Restricted).
- Implement initial data loss prevention (DLP) policies aligned to priority data types and workflows.

Privileged Identity Management for Admin Roles

- Implement time-bound, approval-based role activation; enforce MFA for elevation.
- Define admin role tiers, activation durations, and testing/rollback plans.

Identity Governance — Access Reviews and Entitlement Management

- Implement recurring access reviews for key groups, applications, and privileged roles.
- Use access packages for sensitive SharePoint sites and business-critical apps to automate request/approval/expiry.

Endpoint Privilege Management

- Deploy EPM so users remain standard users while approved tasks elevate just-in-time with audit logging.

Year 5 — Resilience, Optimization, and Long-Term Sustainability

Year 5 outcomes:

- Mature operational practices for Microsoft 365 security and governance with continuous improvement loops.
- SaaS data resilience aligned to the shared responsibility model with a defined backup and recovery strategy.
- Ongoing SaaS app governance and exposure reduction.
- Stable, governed intranet/content platform with lifecycle management and periodic information-architecture refreshes.

Year 5 Workstreams

Microsoft 365 Resilience and Backup Strategy

- Implement a tenant backup strategy aligned to Microsoft recovery scenarios and best practices.
- Perform quarterly restore tests (Exchange, SharePoint, OneDrive) with documented RTO/RPO targets and evidence.

SaaS App Governance and Ongoing Exposure Reduction

- Run quarterly cloud app discovery reviews, policy tuning, and risky OAuth app remediation.

Continuous Improvement Operating Model

- Quarterly security posture and Zero Trust maturity reviews with a prioritized remediation backlog and executive reporting.
- Annual tabletop incident exercises (identity compromise, ransomware, data leakage) to validate response readiness and improve runbooks.

CROSS-CUTTING KPIS

Cross-cutting key performance indicators provide a consistent, measurable way to track progress, risk reduction, and operational health across all initiatives. These metrics inform prioritization, validate outcomes, and support year-over-year improvement.

- Identity security: MFA and SSPR registration completion; legacy authentication sign-ins trending to zero.
- Endpoint compliance: percent of staff endpoints enrolled; compliance rate; patch/update ring success.
- Threat protection: Defender onboarding coverage; email threat policy coverage; identity sensor coverage.
- Content modernization: percent of file shares migrated; intranet adoption; reduction in on-premises storage footprint.
- Security posture: secure score trend and recommendation closure rate.

IMMEDIATE NEXT STEPS — YEAR 1 LAUNCH CHECKLIST

The Year 1 launch checklist identifies the critical actions required to establish foundational security, identity, and endpoint management capabilities. These steps enable controlled pilots, reduce early risk, and set the stage for successful scaling across the Library District.

- Confirm Exchange readiness and complete the hybrid prerequisites assessment.
- Draft Conditional Access baseline (MFA and block legacy authentication) in report-only and define pilot groups.
- Prepare a combined MFA and SSPR registration and launch a registration communications package.
- Build Intune baseline profiles (update rings, security baseline, settings catalog policies).

Current Technology in Use

The Library District uses on-premises Microsoft Exchange for email, legacy open source tools for computer imaging, and Kace for Windows updates. Computers are secured with Fortinet firewall and Palo Alto XDR. The intranet runs on Legacy Adobe ColdFusion on in-house, on-premises servers.

Public Computers

The District provides public-access computing to support research, learning, and community services. Sessions are time-managed during peak-demand periods, with staff assistance available as capacity allows. Usage guidelines emphasize equitable access, privacy, and appropriate use in alignment with District policies.

Printing Capabilities

Self-service printing is available at branches via networked print release. Print management tools help customers authenticate jobs and enable staff to troubleshoot, while promoting responsible and cost-effective use.

Internet Service

The District's wide-area and internet connectivity is provisioned to provide reliable access for staff and customers, supporting cloud services, public computing, and Wi-Fi. Capacity planning, monitoring, and redundancy are used to sustain availability and performance.

Filtering

The Library District applies CIPA compliant content filtering on public-access networks to align with applicable policies, protect minors, and reduce exposure to malicious sites. Processes exist to evaluate requests to review or adjust filtering when educational or research access is unintentionally impacted.

Wireless Access

Secure, open Wi-Fi is provided at branches for customers and visitors with common device types. Network segmentation, authentication controls, and content filtering help protect customers while maintaining ease of access.

Cybersecurity

The Library District implements a multi-layered security approach by utilizing Fortinet firewalls for network protection, Palo Alto XDR for advanced threat detection and response, and Mimecast for email security. Our program focuses on safeguarding systems and data through robust perimeter defense, proactive monitoring, and continuous improvement of security practices.