Ride Connection

Microsoft 365 Engineer with Cloud Infrastructure & Security Architecture

Functions, Tasks, and Full Scope of Duties

Role Element	Description
Department	Information Technology
Reports To	Chief Information Officer
Location	Portland, OR / Hybrid Support Environment
Role Focus	Microsoft 365, Entra ID, Teams, SharePoint, OneDrive, Exchange Online, Intune, Power Platform, Co-Pilot, Cybersecurity, Governance, adoption, and Organizational change management.
Primary Purpose	Train, Configure, Administer, architect, secure, modernize, and support Ride Connection's Microsoft 365 and related technology environment while leading Co-Pilot, Power Apps, SharePoint and Teams adoption, governance, training, and operational support.

1 Response Submission Process and Requirements

The vendor shall prepare and submit a response electronically in Microsoft Word format to **Ride Connection Contracts Division - contracts@rideconnection.org**

The submission deadline is **5:00 p.m. Pacific Time on July 22, 2026**.

1.1 Company Background, History, and Experience

The vendor shall provide an overview of the company, including:

- Legal company name and location.
- Year established and length of time in business.
- Company ownership structure.
- Core services and areas of specialization.
- Experience providing similar professional or technical services.

1.2 Proposed Candidate Resume and Qualifications

The response shall include a current resume for the individual proposed to perform the work.
The resume and accompanying biography should clearly identify:

- Candidate's full name.
- Professional summary.
- Technical, functional, and industry expertise.
- Relevant employment history.
- Experience performing services comparable to those described in the SOW.

1.3 Proposed Hourly Cost

The vendor shall clearly state the proposed hourly billing rate for the candidate. The cost section should include:

Cost Element	Vendor Response
Proposed Candidate	[Candidate Name]
Proposed Role	[Role or Labor Category]
Hourly Rate	$[Amount] per hour

2 Role Purpose and Organizational Context

Ride Connection is modernizing its technology environment to improve secure collaboration, file governance, service delivery, reporting, automation, and operational support across administrative, transportation, NEMT, Mobility Management, Volunteer Management, Finance, HR, Development, Communications, and program teams.

The Senior Microsoft 365 Engineer with Cloud Infrastructure & Security Architecture administers and improves core systems including Microsoft 365, Microsoft Entra ID, Microsoft Co-pilot, safe Artificial Intelligence adoption, Active Directory, Exchange Online, Teams, SharePoint Online, OneDrive, Intune, Power Platform, Power BI, Mobility Management tools, Volunteer Management tools, and other approved business applications.

The role is responsible for secure architecture, operational reliability, access control, collaboration standards, SharePoint and Teams adoption, migration support, automation, endpoint management, service management, documentation, training, and governance. The role also supports modernization efforts that reduce manual work, improve data quality, strengthen cybersecurity, reduce technical debt, and create a better staff technology experience.

3 Key Role Outcomes

- Microsoft 365 environment is secure, well-governed, supportable, documented, and aligned with Zero Trust principles.
- Teams becomes the standard tool for internal communication, active collaboration, meetings, and department workspaces.
- SharePoint/HubCap becomes the primary home for official shared files, organizational digital assets, and governed document storage.
- Staff understand when to use Teams, SharePoint, OneDrive, email, and other approved tools.
- Permissions, ownership, naming conventions, file structures, and retention expectations are clearly documented and consistently applied.
- Identity, access, MFA, Conditional Access, SSO, RBAC, endpoint compliance, and account lifecycle processes are secure and repeatable.
- Adoption barriers, recurring support issues, training needs, access problems, and governance gaps are tracked and resolved through a structured backlog.
- IT leadership receives clear updates on risks, recurring issues, cybersecurity gaps, adoption barriers, vendor concerns, and improvement opportunities.
- Future safe adoption of Artificial Intelligence.

4 Core Functional Areas

Functional Area	Scope
Microsoft 365 Cloud Architecture	Design, configure, secure, and improve Microsoft 365 environments, including Teams, SharePoint, Exchange Online, OneDrive, Entra ID, Intune, Power Platform, and related services.
Identity and Access Management	Administer Entra ID, Active Directory, MFA, Conditional Access, SSO, RBAC, groups, licenses, user lifecycle, access reviews, and least-privilege controls.
SharePoint and Teams Adoption	Lead governance, configuration, file structure, ownership, permissions, training, support, and barrier resolution for Teams and SharePoint adoption.
Infrastructure Migration	Support tenant-to-tenant migration planning, email/PST migration, SharePoint site migration, OneDrive migration, security group mapping, and post-migration validation.
Endpoint Management	Administer Intune, Windows Autopilot, compliance policies, configuration profiles, device security, endpoint standards, and device lifecycle support.
Cybersecurity and Zero Trust	Implement controls related to MFA, Conditional Access, secure access, endpoint protection, phishing awareness, access cleanup, and cybersecurity remediation tracking.
Automation and Scripting	Develop PowerShell scripts, Power Automate flows, Jira automations, alerts, reports, and workflows for provisioning, licensing, audits, access changes, onboarding, and offboarding.
Copilot and AI Readiness	Support Copilot governance, AI security mapping, data readiness, permission hygiene, adoption guidance, and responsible AI practices.
Power Platform and Reporting Support	Support Power Apps, Power Automate, SharePoint Lists, Dataverse, Power BI workspaces, dashboards, data refreshes, and reporting access.
Documentation and Training	Create SOPs, job aids, quick-reference guides, knowledge articles, training materials, governance standards, support procedures, and adoption communications.

5 Essential Functions and Detailed Scope of Duties

5.1 Microsoft 365 Cloud Architecture and Administration

- Architect, deploy, administer, secure, and continuously improve Microsoft 365 environments for organizational collaboration, communication, document management, identity, endpoint management, and productivity.
- Administer Microsoft 365, Exchange Online, Teams, SharePoint Online, OneDrive, Microsoft Entra ID, Active Directory, Intune, Power Platform, Power BI, and related services.
- Design and maintain cloud architecture patterns that support secure collaboration, business continuity, least privilege, data protection, and operational scalability.
- Prioritize Entra ID security, MFA, Conditional Access, role-based access, secure groups, and Zero Trust principles in daily administration and architecture decisions.
- Monitor service health, administrative alerts, licensing, user access, service availability, mail flow, collaboration activity, storage usage, and system risks.
- Maintain configuration documentation, architecture diagrams, ownership records, support procedures, known issues, and escalation paths.
- Coordinate with Microsoft support, managed service providers, vendors, and internal teams when troubleshooting or escalation is required.

5.2 Identity, Access Management, and Zero Trust Security

- Manage user accounts, licenses, permissions, MFA settings, mailboxes, shared mailboxes, distribution lists, Microsoft 365 groups, security groups, dynamic groups, and application access.
- Administer Microsoft Entra ID, Active Directory, SSO, RBAC, Conditional Access policies, authentication settings, access reviews, and secure account lifecycle processes.
- Support onboarding, role changes, transfers, offboarding, and access removal in coordination with HR, IT leadership, and department leaders.
- Implement least-privilege access practices for Teams, SharePoint, OneDrive, Power Apps, Power BI, Jira, RingCentral, and business applications.
- Review and remediate inappropriate access, stale accounts, orphaned groups, unnecessary permissions, external sharing risks, and unmanaged collaboration spaces.
- Escalate suspected cybersecurity incidents, phishing, spoofing, unusual access activity, malware, lost or stolen devices, and unauthorized access attempts.
- Support cybersecurity assessment follow-up, remediation tracking, documentation, access cleanup, account security, and secure device handling.

5.3 Microsoft Teams and SharePoint Governance, Configuration, and Adoption

- Administer and support Microsoft Teams and SharePoint for organizational communication, department collaboration, meetings, channels, document management, file sharing, and user access.
- Configure and maintain Teams, channels, SharePoint sites, document libraries, permissions, metadata, navigation, file-sharing settings, external sharing settings, and collaboration structures.
- Lead SharePoint and Teams adoption scope items, including Phase 1 expectations, governance standards, ownership model, access model, naming conventions, file organization standards, and support processes.
- Define when staff should use Teams, SharePoint, OneDrive, email, Jira, RingCentral, and other approved tools.
- Clarify and train staff on the relationship between Teams channel files and SharePoint document libraries using a practical “same file, two doors” approach.
- Help departments structure Teams, channels, SharePoint sites, document libraries, and folder structures to reduce duplication, improve findability, strengthen security, and align with work practices.
- Assist with migration, cleanup, and organization of shared drive content, local files, and informal file repositories into SharePoint where appropriate.

- Troubleshoot Teams and SharePoint access, meetings, audio/video, notifications, sync, sharing, permissions, files, document libraries, co-authoring, version history, search, and file recovery issues.
- Coordinate with IT leadership to ensure Teams and SharePoint practices align with cybersecurity, records management, privacy, retention, and organizational communication expectations.

5.4 SharePoint File Governance and Migration Support

- Review current SharePoint/HubCap sites, document libraries, folders, permissions, file structures, ownership, and usability concerns.
- Define future-state SharePoint structures for departments, programs, shared resources, official records, templates, forms, operational files, and organizational assets.
- Create and maintain file naming standards, folder/library standards, official record locations, version-control expectations, and document ownership practices.
- Support identification of files to migrate from R: Drive, local storage, OneDrive, email attachments, and other informal locations into SharePoint.
- Plan migration waves, starting with lower-risk shared files and separately piloting complex or sensitive areas such as Finance/fiscal workflows.
- Validate migrated content for access, organization, ownership, version history, searchability, and staff usability.
- Support cleanup of duplicate documents, outdated content, inactive folders, unofficial copies, and unclear file ownership.
- Create guidance for staff on attaching or linking SharePoint files in email without creating unnecessary downloaded copies.

5.5 Endpoint Management and Device Administration

- Administer Microsoft Intune/Endpoint Manager, Windows Autopilot, compliance policies, configuration profiles, device enrollment, application deployment, and endpoint governance.
- Support Windows devices, mobile devices, tablets, phones, printers, peripherals, VPN, MFA, and endpoint connectivity issues.
- Configure and monitor endpoint compliance, device security settings, approved software, patching expectations, device inventory, and configuration standards.
- Support onboarding and offboarding of devices, including setup, assignment, secure wipe, redeployment, and asset tracking.
- Troubleshoot device performance, application access, printer connectivity, user profiles, Teams/SharePoint sync, RingCentral devices, and network access issues.
- Coordinate with vendors and managed service providers for endpoint, network, telecom, or hardware escalations.

5.6 Automation, PowerShell, and Process Improvement

- Develop custom PowerShell scripts to automate user provisioning, license management, audit reporting, account cleanup, group membership reporting, mailbox administration, and access review tasks.
- Use PowerShell, Power Automate, Intune, Jira automation, Microsoft 365 tools, and related technologies to automate routine IT administration and support activities.
- Develop alerts, workflows, forms, notifications, checklists, reports, and support processes for onboarding, offboarding, access changes, license requests, ticket routing, and audit documentation.
- Identify manual processes that can be standardized, automated, integrated, governed, or retired.
- Recommend improvements that reduce manual work, strengthen security, improve reliability, increase auditability, and enhance user adoption.
- Maintain documentation for scripts, workflows, automation logic, dependencies, owners, escalation paths, and support procedures.

5.7 Microsoft Copilot, AI Readiness, and Responsible Adoption

- Support Microsoft Copilot readiness by improving data hygiene, access controls, permissions, governance, information architecture, and staff awareness.
- Apply Copilot Partner Solution Engineer experience to develop practical technical frameworks, adoption guidance, use-case evaluation, and AI security mapping.
- Advise on AI security considerations, including data oversharing, sensitive content exposure, permission inheritance, access reviews, user training, human review, and responsible use.
- Coordinate with IT leadership to align Copilot, AI, automation, and productivity initiatives with cybersecurity, privacy, governance, and business priorities.
- Train users on appropriate Copilot use, prompt practices, data sensitivity, accuracy review, limitations, and approved organizational use cases.
- Support business teams in identifying high-value Copilot and automation use cases that reduce manual effort, improve productivity, and maintain data protection.
- and service changes.

5.8 Power Platform, Reporting, and Business Application Support

- Provide backend operational support for Power Apps, Power Automate flows, Power BI reports, SharePoint Lists, Dataverse, data connections, user access, application permissions, forms, workflows, and business processes.
- Promote governance standards for internally developed applications, including access controls, data protection, documentation, training, supportability, lifecycle planning, and secure sharing.
- Support modernization of manual reporting, Google Docs-based processes, spreadsheets, legacy data tools, and operational workarounds.

5.9 User Training, Documentation, and Adoption Support

- Provide technology orientation and training for Microsoft 365, Teams, SharePoint, OneDrive, RingCentral, Jira Project Management, Jira Service Management, MFA, cybersecurity expectations, devices, and IT support channels.
- Create user-facing job aids, quick-reference guides, training slides, process documentation, knowledge base articles, FAQs, SOPs, troubleshooting guides, and support documentation.
- Conduct demos, office hours, feedback sessions, adoption support sessions, refresher training, and department-specific working sessions.
- Assist users with standard practices for collaboration, document storage, secure access, responsible system use, project tracking, service request submission, and file organization.
- Support rollout of new systems, software updates, endpoint changes, process changes, and modern workplace tools.
- Reinforce clear expectations for when to use Teams, SharePoint, Jira, RingCentral, email, OneDrive, and service desk channels.

5.10 IT Governance, Security, and Leadership Support

- Support IT governance standards for Microsoft 365, Teams, SharePoint, OneDrive, Entra ID, Intune, Jira, RingCentral, Power Platform, SaaS systems, business applications, and endpoint tools.
- Keep IT leadership informed of system risks, recurring issues, adoption barriers, service trends, vendor concerns, cybersecurity gaps, governance gaps, and improvement opportunities.
- Collaborate with IT leadership, HR, Finance, Operations, Development, program teams, vendors, managed service providers, department leaders, and business owners to support technology needs.
- Support system inventory maintenance, application mapping, configuration management, governance standards, modernization planning, and operational technology improvements.
- Mentor or guide help desk staff by sharing troubleshooting practices, documentation, configuration standards, technical knowledge, and user-support expectations.

- Contribute to a secure, customer-focused, well-documented, well-governed, mission-aligned, and continuously improving IT environment.

6 Required Technical Domains and Skills

Domain	Skills / Tools
M365 Ecosystem	SharePoint Online, Microsoft Teams, Exchange Online, OneDrive, Microsoft 365 Admin Center, Power Platform, Power BI, Microsoft Forms, Lists, and collaboration governance.
Identity and Access Management	Microsoft Entra ID, Azure AD/Active Directory, MFA, Conditional Access policies, SSO, RBAC, groups, dynamic groups, security groups, access reviews, and least privilege.
Endpoint Management	Microsoft Intune/Endpoint Manager, Windows Autopilot, compliance policies, configuration profiles, device security, application deployment, and endpoint lifecycle support.
Cloud Architecture and Security	Microsoft 365 architecture, Zero Trust frameworks, Entra ID security, secure collaboration, email security, data protection, external sharing controls, and governance design.
Migration and Infrastructure	Tenant-to-tenant migration, Exchange/PST migration, SharePoint site migration, OneDrive migration, Teams migration planning, security group mapping, and validation.
Automation	PowerShell scripting, Power Automate, Jira automation, audit reporting, provisioning automation, license management, access cleanup, and workflow automation.
Copilot and AI	Microsoft Copilot readiness, AI security mapping, data-permission hygiene, responsible AI guidance, use-case evaluation, and staff adoption support.
Business Applications	Power Apps, Power BI, SharePoint Lists, Dataverse, Mobility Management systems, Volunteer Management systems, Sylogist, ADP, Trip Master, and related operational platforms.
Documentation and Training	SOPs, job aids, quick guides, architecture documentation, governance standards, knowledge management, training delivery, and user adoption.

7 Required Experience

- Three or more years of progressive IT support, systems administration, desktop/endpoint support, cloud administration, or related technology experience; five or more years preferred for senior engineer responsibilities.
- Hands-on experience administering Microsoft 365, Entra ID, Active Directory, Exchange Online, user accounts, permissions, endpoint devices, Teams, SharePoint, OneDrive, Intune, and common business applications.
- Experience architecting and deploying Microsoft 365 environments for SMB, nonprofit, healthcare, transportation, public-sector, or mission-driven service environments.
- Experience implementing Entra ID security, MFA, Conditional Access, RBAC, SSO, and Zero Trust-oriented access controls.
- Experience supporting tenant-to-tenant migrations or major cloud migration activities involving email, SharePoint, OneDrive, Teams, groups, and permissions.
- Experience in creating PowerShell scripts, automations, audit reports, provisioning workflows, license management processes, and access management improvements.
- Experience training users, writing documentation, supporting adoption, and translating technical concepts into clear business language.
- Experience with IT ticketing or service management tools, preferably Jira Service Management or Jira Project Management.
- Working knowledge of cybersecurity practices such as MFA, endpoint security, secure account management, phishing awareness, access reviews, and incident escalation.

8 Other Duties

This independent **Contract** role and scope of duties are not designed to cover or contain a comprehensive listing of all activities, duties, or responsibilities that may be required. Duties, responsibilities, priorities, tools, and activities may change at any time based on organizational needs, technology strategy, cybersecurity requirements, funding, staffing, and operational priorities.