Regional Transportation District

Contracting & Procurement

1660 Blake St.
Denver, CO 80202

Request for Proposals

PROFESSIONAL SERVICES

No. 122DH059

Website Redesign

12/23/2022

REQUEST FOR PROPOSALS
TABLE OF CONTENTS

PART 1

INSTRUCTIONS TO PROPOSERS

INSTRUCTIONS TO PROPOSERS

RFP SUMMARY

A. RFP Schedule

12/23/2022	RFP advertised and made available to prospective proposers.
01/09/2023 1:00 p.m.	Pre-proposal briefing will be held virtually via Microsoft Teams. Please email Ron Bibeau, Purchasing Agent, (ron.bibeau@rtd-denver.com) for an invitational link.
01/17/2023	Inquiry Period: Emailed questions from prospective proposers are to be received by close of business. Questions must be directed to Ron Bibeau, Purchasing Agent at ron.bibeau@rtd-denver.com
01/20/2023	RTD sends responses to written questions, if any, to all prospective proposers via Addendum.
01/30/2023 2:00 p.m. prevailing local time	Proposals due: Emailed proposals must be received by Ron Bibeau, Purchasing Agent, (ron.bibeau@rtd-denver.com).
Week of 02/06/2023	If necessary, oral presentations by selected finalists will be held in an online meeting.
02/14/2023	RTD anticipates making final selection.

B. Work – RTD is seeking proposals from qualified firms to provide a Website Redesign as outlined in the Statement of Work.

C. Cost Type – Payments are anticipated to be made on a **"**Fixed Price" basis.

D. Award of Contract – Award of a Contract from this RFP will be based upon "best value" competitive proposal procedures.

E. Period of Performance – Subject to the Termination provision of the Contract, performance shall commence as of the date specified in the notice to proceed or, if no date is specified, upon Contractor's receipt of notice to proceed, and shall continue for a period of 5 years (inclusive of development, design, implementation and support and maintenance services). If mailed, receipt of the notice to proceed is presumed to be five days after mailing.

F. Options for this Contract – N/A

G. Disadvantaged and Small Business Requirement for Contracts with No DBE/SBE Goal – RTD has not specified a DBE/SBE participation goal for the Work to be performed under the Contract. However, RTD encourages and expects proposers to pursue subcontracting, mentoring, joint venturing, teaming and partnering opportunities with DBE/SBE firms in the ordinary course of its business/teaming strategies. To date, RTD has achieved greater than 20% DBE/SBE participation on its overall FasTracks DBE/SBE Program. Proposers are encouraged and expected to create a level playing field to the maximum practicable extent consistent with the objectives and requirements of the RTD DBE/SBE program based on federal regulations codified at 49 CFR Part 26 and RTD's SBE Program Policy. Therefore, proposers are requested to document their efforts to include DBEs/SBEs in this contracting opportunity, if any. Proposers are also requested to explain in their executive summary how they intend to utilize and/or will encourage subcontracting, mentoring, joint venturing and/or partnering opportunities with DBEs/SBEs for this project. Furthermore, proposers are to submit a general workforce breakdown for their company (including affiliates) and the project specifically **(Enclosure 5: Employer Certification of Workforce**). RTD is interested in your strategies and approach to seeking diversity in the proposer team to include DBEs/SBEs, minorities and women in all phases of subcontracting, supplier and workforce opportunities associated with the Contract. RTD is an equal opportunity employer and also operates a successful Small Business Opportunity Office. Therefore, RTD expects proposers to demonstrate the same meaningful level of commitment to diversity from businesses that participate in RTD's procurement process.

H. Proposals shall be valid for a duration of no less than 90 days from proposal due date.

GENERAL INSTRUCTIONS

A. General.

1. Concise description of the Contract—RTD Website Redesign and Implementation (estimated to be 6-9 months) – and Support and Maintenance of the solution for a period of 5-years.

2. Option(s). There are no Option Periods for this Contract.

3. Requests for approved equals must be received by the Purchasing Agent by email during the Inquiry Period stated in the RFP Schedule. Any request for an approved equal must be fully supported with technical data, test results, or other pertinent information as evidence that the substitute offered is equal to or better than the Specifications requirement. In addition, any test requirements in the Specifications that pertain to an item under consideration for approved equal must be submitted with the request for approved equal. Decisions of RTD shall be reduced to writing by the Purchasing Agent and shall be final. Responses to requests for approved equals will be issued by Addendum per the RFP Schedule date for responses to questions.

4. The Proposal Contents Checklist, Part 2 of the RFP, is included for the proposer's convenience. Each proposer is solely responsible for submitting any necessary forms and certifications that may be required by the RFP.

5. Part 4 of this RFP is a copy of the Contract contemplated for award substantially in the form to be executed.

6. A list of all holders of the RFP is available for view and/or print on the RTD website. The list is obtainable from the RFP advertisement date through the RFP close date.

B. Addenda to RFP. In the event that it becomes necessary to revise any part of this RFP, or if additional information is necessary to enable potential proposers to make an adequate interpretation of the provisions of this RFP, an addendum to the RFP will be provided to each recipient of this RFP.

C. Inquiries. Questions about RTD and this RFP shall be directed, **by email**, to:

Ron Bibeau, Purchasing Agent
Regional Transportation District
1660 Blake St.
Denver, CO 80202-1399
ron.bibeau@rtd-denver.com

1. From the issuance date of this RFP until RTD selects a proposal for award, Ron Bibeau, Purchasing Agent, is the sole point of contact for RTD and RTD's project team members concerning this RFP. (In this RFP and the Contract Documents, this point of contact may be referred to as the Contract Administrator, Contracting Officer, Purchasing Agent, Buyer, or the like.) Any violation of this condition may be cause for RTD to reject the offending proposer's proposal. If RTD later discovers that the proposer has engaged in any violations of this condition, RTD may reject the offending proposer's proposal or rescind its Contract award. Proposers must agree not to

distribute any part of their proposals beyond RTD. A proposer that shares information contained in its proposal with other RTD personnel, RTD project team members, RTD board members, and/or competing proposer personnel may be disqualified.

2. Proposers' questions must be submitted in writing in e-mail submission. All requests for clarifications and/or changes to the form of the Contract, including suggested changes to the Terms and Conditions, must be made during the Inquiry Period. RTD has no obligation to respond to questions or requests for clarifications or amendments that are not submitted in writing, nor to those submitted outside of the Inquiry Period. Except as provided below, RTD's responses to all inquiries properly submitted will be answered in the form of an addendum that will be provided to all recipients of this RFP.

3. If the RFP Schedule provides for a pre-proposal briefing ("Briefing"), RTD will not respond to any questions regarding the RFP until the Briefing. Firms that have received this RFP, whether present for the Briefing or not, will receive: (1) a copy of the minutes; (2) answers to all questions presented; (3) a listing of all recipients of the RFP (current to date of Briefing), and (4) a copy of the sign-in sheet from the Briefing.

PROPOSALS

A. Submission Requirements.

1. Any alteration, insertion, or erasure by the proposer in the form of the RFP documents as originally prepared by RTD shall render the accompanying proposal non-responsive and may constitute cause for rejection. Conditional proposals or those that take exception to the RFP documents or Scope of Work may be treated as non-responsive.

2. Proposal Submission. RTD's Purchasing Agent must receive:

   a) One emailed copy of the technical proposal in Adobe PDF format that is in compliance with The Rehabilitation Act of 1973, 29 USC 701, Section 508, which requires that the document be readable by all, including those with disabilities, and marked as such;

   b) One "Open Records" copy of your technical and cost proposals per the Colorado Open Records Act, C.R.S. § 24-72-200.1 et seq. (as amended), in Adobe PDF format that is in compliance with The Rehabilitation Act of 1973, 29 USC 701, Section 508, which requires that the document be readable by all, including those with disabilities, **marked as such and saved as separate documents**;

   c) One emailed copy of the cost proposal (as a separate file);

   d) One emailed copy of each of the RTD-required submissions contained in Part 2., Forms to be Completed and Submitted with Proposal.

   Your proposal must be received no later than the time and date set forth in the RFP Schedule. Proposals received by RTD after the time and date specified shall be considered non-responsive and shall be returned unopened to the proposer.

3. Signatures. Proposals must be signed by a duly authorized official of the firm. Proposals submitted by consortiums, joint ventures, or teams, although permitted and encouraged, will not be considered responsive unless it is established that all contractual responsibility rests solely with one contractor or one legal entity which shall not be a subsidiary or affiliate with limited resources. Each submittal should indicate the entity responsible for execution on behalf of the consortium, joint venture, or team.
4. Proposal Format.
    a) Technical proposals should not exceed 30 single-sided pages. (One "page" is defined as one standard 8½ x 11-inch sheet of paper in Times New Roman, in no less than 12-point font.) All charts, graphic displays, *etc.*, must be of readable size. Foldouts to illustrate particular items are permitted but will be included in page count. Cover letters should be no longer than two pages.
    b) Submission of standard promotional material and corporate literature not specifically requested by RTD is discouraged. Any such information may not be fully considered in the evaluation.

B. Content Requirements.

1. All proposals must include the signed Addenda acknowledgement included with Part 2, where the proposer should list all addenda received. Failure to provide this acknowledgement form or list addenda may cause the proposal to be rejected as non-responsive.
2. In addition to any information required elsewhere in this RFP and in the Scope of Work, all proposals shall contain and will be evaluated based on the following sections:
    a) A cover letter (**maximum two pages**) briefly describing the firm or firms (including subcontractors, if any) on the proposed project team, referencing the RFP by name and number.
    b) A detailed technical proposal (**maximum 30 pages**) in narrative form describing the proposer and proposed team. Proposals shall include the following items in the order listed below and shall not exceed 30 pages, excluding attachments. Items that will not be counted in the 30-page limit are: the firm's cover letter, résumés, and certifications. Proposals shall address the following:
        (i) Previous experience of the proposed team (including subcontractors) and key personnel in performing on projects of a similar nature and scope.
        (ii) A demonstrated ability to perform under the Contract.
        (iii) A completed Compliance Matrix reflecting response codes from your firm for each of the descriptions/requirements referenced.

c) Supplemental project information appendix, including:

(i) Description, including name of client, of at least two recent projects that demonstrate successful completion of projects of similar nature and scope. Clients may be contacted for references.

(ii) An organizational chart for each firm on the proposed team and résumés for all staff listed on the organizational chart.

(iii) Résumés of all proposed key personnel and the availability during Contract performance periods of all key personnel.

d) Completed forms and certifications required by the RFP.

e) Contract Cost Proposal, as described below.

C. Contract Cost Proposal. Each proposer shall submit, in a separate, emailed document, **one copy only** of the information required below:

1. Cost proposals must clearly identify pricing proposed for the type of Contract to be awarded.

2. All supporting documentation for the cost proposal, including, without limitation:

a) Information demonstrating to RTD that the proposer has the necessary financial resources to perform the Contract. This information should include:

(i) Un-audited balance sheets of the proposer and un-audited balance sheets of proposer and its subsidiaries, if any, for interim quarterly periods since the close of its last fiscal year.

b) Names of banks or other financial institutions with which the proposer conducts business; and

c) Letter of credit commitments (if any).

D. Only One Proposal Accepted. RTD will accept only one proposal for the Work from any one proposer. This includes proposals that may be submitted under different names by one firm or corporation.

AWARD PROCESS

A. Evaluation Criteria. Proposals will be evaluated according to the following criteria, listed in descending order of importance:

1. Cost	30%
2. Technical and Functional specifications of the website including security and data management, implementation strategy and Timeline for completion.	25%
3. Design proposal explaining the research and design phases and approach, and special recommendations for RTD.	25%
4. Experience of firm and key personnel regarding the business needs of RTD as defined.	20%

B. Notification to Successful Proposer. Award decisions of RTD shall be reduced to writing by the Director of Contracting and Procurement, or delegate, and shall be final. RTD will notify the successful proposer, if any, by sending a notice of intent to award, which is subject to any required RTD approval. Following RTD approval, the Contracting Officer will initiate the Contract signature process and then issue the notice to proceed with the executed Contract.

C. Notifications to Unsuccessful Proposers.

1. Pre- and Post-Award Notices of Exclusion. The Purchasing Agent shall notify unsuccessful proposers in writing of exclusion from award. Requests for a debriefing must be submitted to the Purchasing Agent by email within three days of receipt of such notice. Debriefings requested for and provided prior to Contract award shall address only the requesting proposer's proposal; post-award debriefings may address all proposals submitted. Only one pre-award or post-award debriefing shall be provided per proposer.

2. Protests. Protests related to this RFP must be submitted by email to the Purchasing Agent and will only be accepted from proposers whose direct economic interest would be affected by the award of a Contract or failure to award a Contract. Copies of RTD's protest procedures are available upon request to the Purchasing Agent. Proposers must exhaust all administrative remedies prescribed by RTD's protest procedures before proceeding to court.

LEGAL NOTICE TO PROPOSERS

A. Organizational Conflict Of Interest.

1. The proposer shall review the attached Organizational Conflicts of Interest Disclosure Requirements and submit its Organizational Conflicts of Interest Certification with the proposal.
2. If the proposer prepared or assisted RTD in the preparation of a statement of work, work program, or system specifications to be used in a competitive procurement by RTD, the proposer will be ineligible to supply the same in connection with this Contract. The proposer may otherwise compete for RTD business on an equal basis with other parties.
3. Except as provided above, if RTD determines that a potential conflict exists, the proposer shall be excluded from award unless the conflict can be avoided or otherwise resolved through the inclusion of a special Contract provision or other appropriate means.

B. Insurance and Bond Requirements. Proposers' attention is directed to the insurance and bond requirements prescribed in Exhibit 2 to the Terms and Conditions. It is highly recommended that proposers confer with their insurance carriers or brokers in advance of proposal submission to determine the availability of bonds, insurance certificates and any endorsements.

C. News Releases**.** RTD's written approval is required prior to any communication with the press or any public disclosure relating to this RFP or any subsequent awards.

D. Pre-Award Audit**.** RTD reserves the right to conduct a pre-award audit to verify labor rates, overhead rates, *etc*. should RTD determine that such an audit is required prior to negotiation or award of a Contract.

E. Cost of Proposal Preparation**.** RTD shall not reimburse proposers for costs incurred for preparation of proposals or required documentation.

F. Materials Submitted**.** All materials submitted shall become the property of RTD and will not be returned to the proposer.

G. Confidentiality**.** RTD is a public entity subject to the provisions of the Colorado Open Records Act, C.R.S. § 24-72-200.1 et seq. ("CORA"), and all materials submitted with this RFP, with the exception of trade secrets, privileged information, and confidential commercial, financial, geological, or geophysical data pursuant to C.R.S. § 24-72-204(3)(a)(IV), may become public records subject to inspection by the public at any time after the Contract is executed. Therefore, any confidential or proprietary information that the proposer discloses to RTD with respect to this RFP must be clearly designated as confidential or proprietary at the time of disclosure by the proposer to RTD. RTD shall not disclose properly designated information unless such information is required to be disclosed by law or court order. In the event of a legal challenge to the confidentiality of records so designated by the proposer, RTD shall make reasonable efforts to notify the proposer prior to disclosing any such information, and in some cases may tender to the proposer the defense of any action filed. By submitting a proposal under this RFP, the proposer agrees to accept such tender of defense and in all cases assumes exclusive

responsibility for defending its position as to the confidentiality of the requested information. RTD is not obligated to assist in such defense, and cannot and does not guarantee that the confidentiality of records so designated will be upheld by a reviewing court. **If the proposer fails to submit a copy of its proposal that may be released under CORA, the proposer acknowledges that RTD has the authority to disclose, and may disclose in its discretion, any non-designated information contained in the proposal in response to a CORA request.**

H. Rights Reserved to RTD.

1. All proposers are notified that the execution of a Contract pursuant to this RFP is dependent upon negotiation of a mutually acceptable Contract with the successful proposer(s) and subsequent appropriation by RTD's Board of Directors of the necessary funds. **Successful proposers must be prepared to execute the Contract (as may be amended by the issuance of Addenda) that is provided with this RFP. RTD has no obligation to accept requested changes to the form of the Contract terms beyond the Inquiry Period, and no changes will be made after award to the successful proposer(s) (other than in respect of typographical errors).**
2. It is the intent of RTD to make an award within 60 days from the proposal due date; however, all proposals shall be valid for no less than 90 days.
3. RTD reserves the right to reject all offers and re-solicit or cancel this RFP if deemed by RTD to be in its best interest.
4. RTD reserves the right to enter into a Contract with any proposer based upon the initial proposal or on the basis of a best and final offer without conducting oral discussions.

I. Prohibited Interests. No employee of RTD or any member of its governing body shall have any personal or financial interest, direct or indirect, in this Contract or any contract executed subsequently in connection with this Contract during his or her tenure or for one year thereafter. No director, officer, employee, or agent of RTD shall be interested in any contract or transaction with RTD except in his or her official representative capacity.

J. Competition in Subcontracting. Proposers shall select subcontractors (including suppliers) on a competitive basis to the maximum practicable extent consistent with the objectives and requirements of any Contract awarded.

K. Personnel Availability. By submitting its proposal, the proposer certifies that it and each of its subcontractors possess an adequate supply of workers qualified to perform the work specified within the Contract schedule; that there is no existing or impending dispute between it and any labor organization; and that it is prepared to comply fully with prevailing wage requirements, minimum wages, maximum hours of work, and equal opportunity provisions contained in the Contract Terms and Conditions.

PART 2

PROPOSAL CONTENTS CHECKLIST

PROPOSAL CONTENTS CHECKLIST

Your submitted proposal must contain the following items in emailed form, in this order. See the Instructions to Proposers (Part 1) for details.

- ☐ Cover Letter (Maximum 2 Pages)
- ☐ **Addenda Acknowledgement Form**
- ☐ Technical Proposal (Maximum 30 Pages)
  - ☐ One copy of the technical proposal, including completed Compliance Matrix, in Adobe PDF format that is in compliance with The Rehabilitation Act of 1973, 29 USC 701, Section 508, which requires that the document be readable by all, including those with disabilities, and marked as such.
  - ☐ One "Open Records" copy of your technical proposal, including completed Compliance Matrix, per the Colorado Open Records Act, C.R.S. § 24-72-200.1 et seq. (as amended) in Adobe PDF format that is in compliance with The Rehabilitation Act of 1973, 29 USC 701, Section 508, which requires that the document be readable by all, including those with disabilities, marked as such
- ☐ **Cost Proposal Worksheet** (submitted as a separate file)
- ☐ **Compliance Matrix**
- ☐ **Certification Regarding Organizational Conflict of Interest**
- ☐ **W-9 Taxpayer Identification Number Request Form**
- ☐ **Solicitation Statistics**

*** Items In Bold Have Been Provided.**

ACKNOWLEDGMENT OF ADDENDA RECEIVED

The undersigned acknowledges receipt of the following addenda to RTD Request for Proposals documents (give number and date of each):

Addendum Number _____ Dated: _____

Addendum Number _____ Dated: _____

Addendum Number _____ Dated: _____

Addendum Number _____ Dated: _____

Addendum Number _____ Dated: _____

Addendum Number _____ Dated: _____

Failure to acknowledge receipt of all addenda may cause the proposal to be considered non-responsive to the request, which would require rejection of the proposal.

The undersigned understands that any condition stated above, clarification of the above, or information submitted on or with this form other than requested will render the proposal non-responsive.

Proposer Name: _____

Address: _____

_____

By: _____

Signature of Authorized Official
Title:
Date:

Regional Transportation District
Solicitation #122DH059
Attachment A - Cost Submittal Form - Sample
Website Redesign

NOTE: This Cost Submittal Form, in Excel format (attached) , must be used to submit pricing for RFP 122DH059

Company Name: *Enter Company Name Here*
Date Submitted: *Enter Submittal Date Here*
Contact Name : *Enter Contact Name Here*
Contact Email: *Enter Contact Email Here*

Task	Unit	Qty	Cost	Description
Task 1: Implementation Phase 1	LS	1		Website Design, Architecture, Content
Task 2: Implementation - Phase 2	LS	1		Development of Website
Task 3: Software Subscription	LS	1		Content Management System
	Hourly Rates	Hours	Estimated Cost	
Task 3: Services and Maintenance Year 1	$0.00	400	$0.00	Services and Maintenance
Task 4: Services and Maintenance Year 2	$0.00	400	$0.00	Services and Maintenance
Task 5: Services and Maintenance Year 3	$0.00	400	$0.00	Services and Maintenance
Task 6: Services and Maintenance Year 4	$0.00	400	$0.00	Services and Maintenance
Task 7: Services and Maintenance Year 5	$0.00	400	$0.00	Services and Maintenance
TOTAL (TASKS 1 - 7)		2,000	$0.00	

All items to be quoted as FOB: Destination

Signature: (Electronic Signature is Acceptable)
Printed Name:
Title:
Date:

In compliance with the above and attached information, the undersigned offers and agrees, if acceptance of this quotation shall be received within 90 days of the above date for receipt of quotations, to furnish the products and/or services described, at the price or prices set forth in this quotation, within the time limitations specified in the schedule and/or the attachments to this quotation.

This Requirements Compliance Matrix form must be completed and submitted with your proposal. *Note: Please refer to the RFP Statement of Work, Section 4, for additional Project Requirement information.* **Instructions:** For each table of requirements listed below please respond with one of the following response codes:	**Company Name:** *Please enter Company Name Here* **Date of Proposal:** *Please enter Proposal Date Here*

Response Code	Definition
FC	**Fully Compliant** – Proponent fully complies with requirement. Responses that are qualified by exceptions or limitations, etc. in the Compliance Matrix shall be considered the equivalent of "NC" (does not comply).
CM	**Complies with Modified Requirement** – Proponent shall provide modified requirement language to which they commit to comply. The "CM" shall be equivalent to a response of "FC" if RTD opts to change the requirement as proposed, or to a response of "NC" if RTD opts to not change the requirement. If complete alternate requirement wording is not proposed in conjunction with a "CM" response, the response shall be considered equivalent to a response of "NC" to the requirement as stated in the RFP. RTD alone shall be the judge of the completeness and appropriateness of alternate requirement language.
NC	**Does Not Comply** – Proponent does not comply with the requirement. Accompanying comments are discouraged. .

ID	Name	Type	Description	Response Code	Comments
REQ-1	Stakeholder Engagement	Business	Contractor shall engage the various stakeholder groups (provided by RTD) to determine end-user business needs.		
REQ-2	eAccessibility	Functional	Initial design shall consider common web accessibility (eAccessibility) practices that allow for easy site navigation for users with disabilities and also consider socio-economic restrictions to bandwidth and speed. Site design shall adhere to Web Content Accessibility Guidelines (WCAG) version 2.1 recommendations. Wesbite implementation deliverables shall utilize Progressive Enhancement (PE), Landmark Elements for assistive technology, Semantic HTML, accessible defaults, accessible routing, and include an accessibility statement.		
REQ-3	CMS Browser Compatibility	Functional	CMS site adminstration must be accessible from any modern internet browser.		
REQ-4	Content Repository/Archiving	Functional	Previously published content, images and associated data shall be accessible to administrators of the site with minimal effort required for retrieving (i.e. keyword search). Additionaly, historical page revisions shall be accessible to site administrators indefinitely via the CMS.		
REQ-5	Document Updates	Functional	RTD requires easy-to-update documents that are modified with new content frequently. This includes, but is not limited to, the Board of Directors subpage (https://www.rtd-denver.com/board-of-directors), financial data (https://www.rtd-denver.com/financials-investors#financial-documents) and the News Stop section (https://www.rtd-denver.com/news-stop)		
REQ-6	Content Owner Roles	Functional	RTD content owners responsible for applicable site subpages must be able to operationally manage content for their specific pages of the website (i.e. a news stop https://www.rtd-denver.com/news-stop)		
REQ-7	Optimal Performance Measures	Functional	See Appendix A for a list of performative metrics that RTD requires for the future website.		
REQ-8	Queued Content Updates	Functional	The preferred solution shall allow for the ability to preschedule content updates or to set a regular schedule (i.e. weekly) for automated changes. A date picker feature shall be incorporated for pre-loading and scheduling content to go-live at a future scheduled time and date.		
REQ-9	Real-time content preview	Functional	The preffered solution would allow RTD content managers to preview changes before publishing them to the site.		
REQ-10	Responsive Site Loading	Functional	The solution must provide responsive site loading, including page speed. Contractor shall provide evidence that solution is built for optimal performance.		
REQ-11	Content Templates and Scalability	Functional	Solution shall allow for rapid creation of new content (i.e new pages). Contractor shall collaborate with RTD stakeholders to establish a scalable content strategy and repeatable workflow. Solution shall have the option to drag and drop content and images once templates and styles are established.		
REQ-12	Custom User Roles	Functional	The solution must allow for provisioning custom user roles for ease in managing specific content or working in the code base.		
REQ-13	User-Centric	Functional	The redesigned public website (rtd-denver.com) shall focus on customers' transit and other needs and interactions and shall include such elements as enhanced search functionality and accurate and easy-to-use website navigation layout. End-users shall have easy access to up-to-date information, trip plans, schedules, new routes, etc.		
REQ-14	Versioning	Functional	Solution shall allow for the ability to rollback current page builds to previous versions for production.		

REQ-15	Web Browser Compatibility	Functional	Site will work seamlessly across all major web browsers.		
REQ-16	Language Translations	Functional	Solution must support integrating a translation/localization option to allow site content to be submitted and translated into English, Spanish and (potentially) Simplified Chinese languages.		
REQ-17	Codebase Rewrite	Technical	The contractor, along with RTD's front-end developers, shall rewrite RTD's existing codebase for the existing 300-page marketing website (HTML/CSS/Javascript/PHP and Drupal's Drush) to work with the future solution that will continue to be housed in RTD's instance of GitHub. The new codebase shall incorporate modern front-end languages, e.g., JS, React, HTML, JSX, CSS		
REQ-18	CMS/API Delivery	Technical	RTD content that is housed in the headless CMS will have the ability to be delivered via Application Programming Interface (APIs) for seamless display across various desktop, tablet and mobile devices.		
REQ-19	CMS Hosting/Content Infrastructure	Technical	CMS and hosting of associated content shall be cloud-based and utilize microservices architecture. The content infrastructure shall allow for cross-collaboration and for developers to work in parallel as a team utilizing an Agile framework. Content infrastructure shall allow ease of reusability for content creation.		
REQ-20	Decoupled Solution	Technical	The solution shall be a decoupled application utilizing JAMstack architecture with separate front and back ends that allow content edits and development work to occur asynchronously.		
REQ-21	Github	Technical	A competitve solution shall provide seamless integration with GitHub's software and associated version control tool Git.		
REQ-22	React and JAMstack achitecture	Technical	A competive solution shall utilize a React and Javascript, APIs, and Markup (JAMstack) framework to provide the website experience.		
REQ-23	Cloudfare integration	Technical	Solution shall be compatible with Cloudfare (RTD's current middle tier solution).		
REQ-24	URL Redirection	Technical	Solution shall uphold all URL redirects that are in place for the current website.		
REQ-25	Next Ride Application Integration	Technical	The new site shall incorporate RTD's recently built Next Ride application (https://beta.rtd-denver.com/) and contractor shall ensure it appears to end-users as part of the same site (look and feel, URL). Next Ride is built in Next.JS using React with the Chakra UI component library.		
REQ-26	CMS Browser Extension	Technical	The recommended CMS solution shall allow for Chrome or similar extenstion to be used by content owners of specific pages of the site to edit and deploy content.		
REQ-27	API Endpoints	Technical	The solution shall use all API endpoints existing on the current site (to be shared by RTD) in the development of the new website.		
REQ-28	Analytics Platform Integration	Technical	Vendor shall integrate solution with RTD's existing analytics platforms Google Analytics 4 (GA4) and Google Tag Manager (GTM).		
REQ-29	Existing Application Lookup Integration	Technical	Contractor shall develop a strategy and migrate existing lookup applications, including but not limited to: RTD's License Plate Lookup, Access-A-Ride, Board of Directors District Lookup, and Flex Ride service area.		
REQ-30	Component libraries	Design	Solution shall create reusable components to be utilized by RTD content creators throughout the site (i.e. updating a local fare token in one section of the site automatically updates fare postings throughout the site).		
REQ-31	Design Systems	Design	The collection of tools, platforms, applications and software that comprise the new technology stack shall be complementary of one another.		
REQ-32	Developer Experience (DX)	Design	The solution shall provide easy maintainability and debuggability, hot reloading of content, declaritive rendering, componentization, declarative data queries, asset pipelines, Cascading Style Sheets (CSS) extensions, modern JS syntax and require a low level of effort for developers.		
REQ-33	RTD Brand Standards	Design	Redesign shall match RTD brand standards located at https://www.rtd-denver.com/brand-elements, while proposing guideline enhancements that visually connect with our audience.		
REQ-34	Mobile-First Design	Design	The site shall be designed to be viewed on mobile devices first, while also maintaining best-in-class design and functionality on laptops and desktops. Site shall work seamlessly across modern browsers on widely-used smartphones, tablets and associated Operating Systems (OS).		
REQ-35	Scope of Design Services	Design	Design services shall include a path from initial concepts to functional prototypes.		
REQ-36	Search Engine Optimization	Design	The solution shall incorporate web design practices and integrations that align with industry-leading search engine optimization (SEO).		
REQ-37	Usability	Design	Product must be easy to use for RTD internal users who do not have technical expertise		
REQ-38	Notification Banner	Design	Solution shall include notification banner options on the site homepage for displaying messages to website visitors. Additionally, RTD needs the ability to display systemwide notifications with varying colors, depending on the message type. For example, success (green), information (blue), warning (orange), error (red), disabled and compact (grey).		
REQ-39	Form Builder	Design	Solution shall allow for the use of a form builder to pass information to RTD's Salesforce backend solution.		

REQ-40	Image Size Editing	Design	The CMS shall allow for direct editing of image sizes to be dsplayed on landing pages within the CMS.		
REQ-41	Reusable UI Components	Design	Solution shall provide Image Component and Image Optimization using Next.js		
REQ-42	Template Options	Design	Contractor shall deliver multiple template options to differentiate page layout, structure, and design throughout the site.		
REQ-43	Kick-off Meeting	Project Management	A Project Kickoff Meeting, coordinated with the RTD Project Manager, shall be scheduled within seven (7) days after Notice to Proceed (NTP) and conducted within twenty one (21) days. The Project Kickoff Meeting will be conducted by the Contractor and the RTD Project Manager at RTD offices, through Microsoft Teams, or other high-quality teleconferencing approach.		
REQ-44	Project Meetings	Project Management	The RTD Project Manager shall schedule and facilitate Progress Meetings held between the Contractor and the RTD on a weekly or every other week basis, as deemed necessary by the RTD, for the purpose of reviewing progress, coordinating activities, and other project activities that cannot be resolved by correspondence. The timing of these meetings shall be conducted at the RTD's sole discretion, based on the nature of the current project activities. These meetings may be at RTD offices, through Microsoft Teams, or other high-quality teleconferencing approach.		
REQ-45	Project Meeting Agendas	Project Management	Agendas for the Progress Meetings will be prepared by the Contractor and may include any topics that the Contractor's Project Manager determines to be relevant to the project. The Contractor shall insure that persons knowledgeable in the topics to be discussed, including subcontractors, subject matter experts, and/or technical representatives, are present at all necessary meetings. Agendas will be submitted at least two (2) business days prior to the meeting.		
REQ-46	Meeting Summaries	Project Management	Meeting summaries shall be taken at all meetings. Summaries shall include a summary of all topics discussed, a listing of all understandings and agreements reached, and an updated Action Item List (AIL). Unless otherwise agreed, the Contractor shall be responsible for taking all meeting summaries. The format for the meeting summaries shall be developed based on input from the RTD.		
REQ-47	Meeting Summaries	Project Management	The meeting summaries shall be distributed to all attendees for review within three (3) business days from the end of the meeting.		
REQ-48	Action Item List	Project Management	During meetings, action items will be identified, with each action item assigned to an individual for disposition by a pre-determined response date. These action items shall be maintained and updated throughout the project by the Contractor, in an Action Item List (AIL). The AIL format will be mutually agreed upon by the Contractor and the RTD.		
REQ-49	Issue Tracking systems	Project Management	The Contractor shall provide RTD key personnel access to any issue tracking system used by the Contractor for Sprint planning during the project. The Contractor will provide no less than monthly a status report of all tickets.		
REQ-50	Monthly Status Report	Project Management	Contractor shall provide to the RTD PM a status report monthly highlighting key accomplishments, risks, issues, and milestones/deliverables updates.		
REQ-51	Invoice Documentation	Project Management	The Contractor shall keep and maintain reasonably complete and reliably detailed records of milestones achieved in performing the Contract, including records of productivity to identify basis for payment, sufficient to evaluate the accuracy, completeness, and currency of the costs or prices.		
REQ-52	Project Schedule	Project Management	Within thirty (30) days after Notice to Proceed (NTP), the Contractor shall furnish, to the RTD for the RTD's approval, a detailed Project Schedule. The detailed Project Schedule shall be based on critical-path-method and constructed using Microsoft Project or RTD approved substitute.		

REQ-53	Project Schedule	Project Management	The detailed Project schedule shall show start and completion of the work with dependencies for each activity and shall be properly ordered and sequenced. It shall identify all major work tasks including critical events of design, procurement, delivery schedule, installation, testing, and integration, and shall identify interface activities, subcontractor contributions and submittals, RTD inspections, tests, and approvals as may be required by this document, additional details shall be provided, such as: · A clear description of the activity, including its location · The duration expressed in full working days · A responsibility for work denoting the Contractor, a subcontractor, RTD, or entity performing the activity · The quantity of material, in units · Type of equipment needed (if significant or unusual) · The integer percent complete representing the installed progress · The actual start and finish dates when applicable Requirements and events which impose limitations, as well as dates and milestones which constrain the time, shall be clearly identified.		
REQ-54	Personnel	Project Management	All personnel assigned by the Contractor must display appropriate identification while on RTD property and must adhere to all RTD Rules and Regulations.		
REQ-55	Project Schedule Updates	Project Management	The Contractor shall be required to submit project schedule updates on at least a monthly basis. More frequent near-term schedule updates may be required, if deemed advantageous by the RTD for monitoring the progress of specific phases of the project.		
REQ-56	Project Communications	Project Management	Within thirty (30) days of Notice to proceed (NTP), the Contractor shall provide a RACI along with Contractor's escalation procedure, including contact names and information for each level of escalation.		
REQ-57	Project Communications	Project Management	The Contractor shall promptly notify the RTD PM of any problems or difficulties that may affect the timely or effective completion of the project or any scheduled deliverables.		
REQ-58	Project Communications	Project Management	The Contractor shall coordinate activities with RTD PM regarding affected RTD business units and personnel, and with external individuals and organizations.		
REQ-59	Subject Matter Experts	Project Management	The Contractor shall make all subject matter experts available - when required or requested.		
REQ-60	Quality Assurance	QA	The Contractor shall plan, establish, and maintain a Quality Assurance (QA) program. The Contractor's QA program shall be imposed upon all entities within the Contractor's organization and on all subcontractors whenever contract work is performed.		
REQ-61	Quality Assurance	QA	A QA Program Plan shall be submitted for review within 30 days of Notice to Proceed (NTP). The QA Program Plan shall describe the methods for planning, implementing, and maintaining quality, schedules, and cost. The QA Program Plan shall contain a company policy statement that clearly defines the authority and responsibilities of QA personnel.		
REQ-62	User Role Training	Training	Contractor shall provide training for all hands-on roles for maintaining the platform utilizing RTD's implementation, where practical.		
REQ-63	CMS Support & Maintenance	Support_Maintenance	Contractor shall provide on-demand support as requested from RTD based on a retainer work order contract. RTD resources must be able to manage and support normal operations after website go-live. Contractor to include a quote in the RFP response for an initial 1, 000 support hours retainer, to include the hourly bill rate. RTD anticipated support needs may include future custom development, assistance with large system upgrades and technical troubleshooting.		
REQ-64	Documentation	Documentation	All documentation shall be in English, shall utilize Imperial measurements, and shall be submitted directly to RTD electronically in the following formats, as applicable: MS Office formats (DOC, XLS, PPT, VSD) Adobe PDF (searchable) Scanned documents consisting of signatures, etc. may be approved for submittal		
REQ-65	Documentation (Manuals)	Documentation	The vendor shall provide written detailed system operation, administration, configuration, architecture, and maintenance manuals to RTD. Manuals shall be complete, accurate, and up-to-date, and shall contain only information that pertains to the system(s) installed.		
REQ-66	Documentation	Documentation	All pages of the documentation shall carry a title, version number and issue date. All manuals shall contain a complete subject index.		
REQ-67	Documentation	Documentation	Documentation shall require re-issuance if any change or modification is made to the system proposed to be supplied. The Contractor may re-issue individual sheets or portions of the documentation that are affected by the change or modification. Each re-issuance or revision shall carry the same title as the original, with a change in version number and issue date.		

REQ-68	Documentation	Documentation	Approved documentation shall be a condition of final acceptance, and updated documentation will be required at any time the Contractor provides software or hardware upgrades. If the documentation as submitted is found to be unacceptable due to incompleteness or inaccurate information, the documentation shall be returned to the Contractor for corrective action and resubmitted for acceptance prior to the release of Final Acceptance payment.		
REQ-69	Documentation	Documentation	The Contractor shall provide Interface Control Document (ICD) and Entity Relationship Diagram (ERD) for all interfaces.		
REQ-70	Collaboration Tools	Documentation	The Contractor shall use RTD's Microsoft Team Site for document sharing/repository.		
REQ-71	System Recovery Plan	Documentation	The Contractor shall provide a system recovery plan detailing the procedures and timelines in ensuring system operability is restored within 24 hours.		
REQ-72	System Implementation Plan	Documentation	The Contractor shall develop a System Implementation Plan (SIP) no less than 60 days prior to start of system implementation. The SIP describes how the System will be installed, deployed and transitioned into an operational System. The SIP will contain an overview of the System, a brief description of the major tasks involved in the implementation, assumptions, constraints, risks, the overall resources needed to support the implementation effort (e.g., hardware, software, facilities, materials, and personnel), and the cutover plan to transition to the new System with minimal adverse impact to RTD's operations. The overall sequence and site-specific implementation specifications will also be documented. The SIP must be approved by RTD prior to its implementation.		
REQ-73	Cross-Collaboration	Personnel	RTD developers shall work with contractor developers in sprints throughout the project to understand how to manage and work with the new code repositories and CMS.		
REQ-74	Joint Design and Development Collaboration	Personnel	Contractor shall collaborate with RTD designers and developers on the new site design.		
REQ-75	Migrate RTD Legacy Content Repository	Product_service	The current website contains numerous images, PDFs, videos and files stored on the existing CMS. Contractor shall facilitate migration of the legacy content onto the new CMS.		
REQ-76	Minimum Viable Use	Security	The product(s) created and purchased for this solution shall have a minimum viable use of three (3) years from the date of purchase. Products that are end of life or scheduled for sunset within three years of the date of purchase are ineligible. Should the product purchase be part of an overarching service contract that includes the ongoing purchase, installation, and maintenance of commercially-available equipment over a fixed term, purchased products must be replaced when they reach end-of-life status.		
REQ-77	Patches and Upgrades	Security	Should the product include software or firmware components, to maintain the currency, supportability, and security of the product software or firmware, the product shall be accompanied by a maintenance or licensing agreement that shall, at minimum, include patches for security and bug fixes (including roll up packages for updates, e.g. service packs) and incremental version upgrades for no less than three consecutive years from the installation date.		
REQ-78	Implementation Guide	Security	The product shall be accompanied by clear and unambiguous written instructions (e.g. a manual or product implementation guide) on how to set security features for the product. At minimum, the instructions shall address access control features, including changing of default user IDs and passwords post-installation and managing encryption keys (as applicable). For networked products, the instructions shall additionally include a list of the minimum necessary services, ports and protocols required to facilitate communication between this product and others (e.g. a database server).		
REQ-79	Responsible Sourcing	Security	Products with Department of Homeland Security directives against purchase or that are sold or manufactured by companies on the Department of Labor Office of Federal Contract Compliance Programs Debarred Companies list are ineligible. Additionally, to the extent that it is possible to provide, the Contractor shall provide RTD with additional information about the manufacture or acquisition of safety or security sensitive products to ensure they are responsibly sourced and reduce the risk of embedded threats and vulnerabilities.		
REQ-80	Logging	Security	The product shall support or facilitate logging and forwarding of application security events for operational failure, security incident, and security monitoring purposes.		
REQ-81	Access Control and Authority	Security	The product shall contain features that allow administrators to control user and system access to functions, features, or system components a need-to-know basis. The product must be able to operate with user level authority, and must not require that a user be logged in as an administrator in order to operate properly. Users and administrators of the product must be able to change and otherwise manage their credentials (for example, establish a password and perform password resets).		

REQ-82	Data Security	Security	Products that are intended for the storage, processing, or transfer of sensitive data shall support strong encryption at rest. Products that communicate over the Internet, for example, for authentication, maintenance purposes, or remote management, shall use unbroken encrypted communication methods. Products that store sensitive data shall tolerate and/or enforce purging data that RTD determines no longer has a business need to be retained.		
REQ-83	Proof of Concept	Security	Proof of concept systems and environments shall be physically and logically separate from RTD production systems and shall not require the use of any production RTD data.		
REQ-84	Exceptions	Security	Should a product be necessary to fulfill the scope of services under the Agreement, yet incapable of conforming to some or all of the aforementioned requirements, the Contractor shall identify the non-conforming product to RTD and the specific requirements that are not met to afford RTD the opportunity to understand the risks to RTD's operations. The Contractor shall additionally explore and present alternatives, including but not limited to use of a different product, configuration options, or other risk mitigation measures, and present those opportunities to mitigate risk (if any) to RTD. The Contractor shall not install a non-conforming product without RTD's written approval.		
REQ-85	Control Activities	Security	At RTD's request, Contractor shall provide RTD the opportunity to review the design and execution of the control activities performed by the Contractor as relates to the support and security of RTD's operations and the data, systems, networks, or facilities that are relevant to providing services to RTD (as applicable to the scope of services).		
REQ-86	Disaster Recovery and Business Continuity	Security	Contractor shall maintain and implement a disaster recovery plan to ensure continuity of the services provided to RTD pursuant to this Agreement and the recovery of any data or functionality lost due to operator error, system error or other unforeseen circumstances. Upon written request, Contractor shall provide RTD with a copy of its current disaster recovery plan and all updates to these plans during the term of this Agreement. In addition, Contractor shall maintain and implement a business continuity plan for the term of this Agreement. Upon RTD's written request, Contractor will issue to RTD a summary statement on the design of the business continuity management framework. The Business Continuity Plan is confidential and Contractor will not provide actual plans nor will it allow customers to participate in business continuity activities.		
REQ-87	Multi-Tenancy	Security	Should a multi-tenancy architecture be used, Contractor shall implement and maintain access controls to adequately separate the functions of each environment such that actions taken in or for another customer do not affect the security of RTD's data or operations on the same architecture.		
REQ-88	SOC 2 Type 2 Report	Security	Fourteen calendar days after receipt of the NTP, Contractor shall provide to RTD their most recent Service Organization Control (SOC) 2 Type 2 report pertaining to the scope of services provided to RTD. Thereafter, for the term of this Agreement, the Contractor shall provide an updated SOC 2 Type 2 report to RTD on an annual basis. If Contractor fails to provide an updated SOC 2 Type 2 report, then Contractor will notify RTD in writing of a date when the SOC 2 Type 2 report will be made available to RTD, except that the updated SOC 2 Type 2 report must be made available to RTD no later than 18 months after the last report was produced. If Contractor's SOC 2 Type 2 report is qualified, then Contractor will provide a written Plan of Actions and Milestones to notify RTD of what actions they are taking to correct any findings and the expected resolution date for those corrections. Should a SOC 2 Type 2 not be performed or available, an alternative third-party control audit report may be acceptable to RTD with prior notice, sufficiency of criteria		
REQ-89	Risk Assessment	Security	Contractor shall perform a risk assessment prior to any major system change or installation that impacts the storage, collection, transmission or processing of RTD Data, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting RTD Data, or changes in security controls related to RTD Data. Identified risks and mitigation plans must be reviewed with RTD prior to change implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.		
REQ-90	Vulnerability Testing	Security	Contractor shall perform a risk assessment prior to any major system change or installation that impacts the storage, collection, transmission or processing of RTD Data, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting RTD Data, or changes in security controls related to RTD Data. Identified risks and mitigation plans must be reviewed with RTD prior to change implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.		
REQ-91	Recovery Point Objective (RPO)	Security	Data backups shall occur no less frequently than once every (12) hours.		
REQ-92	Recovery Time Objective (RTO)	Security	The amount of downtime for a system outage shall not exceed (60) minutes.		

REQ-93	Single Sign-On (SSO)	Security	Software shall be capable of SSO integration with Microsoft Azure for developer access.		
REQ-94	Multi-Factor Authentication (MFA)	Security	Software shall be compatible with widely available Two-Factor Authentication (2FA) technology.		
REQ-95	Transport Layer Security (TLS) Encryption	Security	Solution shall be capable of encryption in transit with TLS version 1.2 or higher.		
REQ-96	Certificate Authority (CA)	Security	Website security certificates shall be managed and maintained by the Contractor.		
REQ-97	Content Management System (CMS)	Product	Contractor shall propose a Content Management System solution to replace RTD's current Drupal-hosted CMS with a modern, easier-to-use platform. Contractor's proposed solution must be fully capable of supporting React-based websites.		
REQ-98	Headless Content Management System (CMS)	Product	Contractor shall propose a headless CMS solution where the content repository “body” is separated or decoupled from the presentation layer “head.”		
REQ-99	Content Migration	Product	The Contractor solution must have the functional ability to migrate content from the current CMS to the future solution. Contractor shall provide resources to implement content migration from the legacy RTD website to the new site based on total amount of content (RTD's current site has approximately 350+ pages).		
REQ-100	Design Deliverables	Product	Contractor shall provide documentation related to managing and updating the site including but not limited to: landing page style guide, taxonomies, necessary resources to edit the site, user flow diagrams, brainstorming notes, etc. Page architecture and elements will follow UX principles in displaying content clearly, prominently displaying call to actions (CTAs), headings, etc.		
REQ-101	User-Friendly Content Management System	Product	The solution must use a CMS that does not require coding or speacilized skill sets to make changes to content.		
REQ-102	Contractor References (sites)	Product	Contractor will provide (3) examples of site designs of similar size and scope to RTD's current site.		
REQ-103	Content Delivery Network (CDN)	Product	Vendor, with RTD agreement, shall recommend a CDN to implement.		

ORGANIZATIONAL CONFLICTS OF INTEREST DISCLOSURE REQUIREMENTS

(a) Organizational conflict of interest means that, because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to RTD, or the person's objectivity in performing the Work is or might be otherwise impaired, or a person has an unfair competitive advantage.

(b) Each firm responding to the RFP shall provide the statement described in paragraph (c). This requirement will apply individually to any of the firm's consultants or lower-tier subcontractors that also furnish Work in performance of the Contract to be awarded.

(c) The statement must contain the following:

(1) Name of the firm and the number of the RFP in question.

(2) The name, address, telephone number, and federal taxpayer identification number, if applicable, of the firm.

(3) A description of the nature of the Work rendered by or to be rendered on the Contract or related to the Contract.

(4) A statement of any past (within the past 12 months), present, or currently planned financial, contractual, organizational, or other interests relating to the performance of the Contract. For contractual interests, such statement must include the name, address, and telephone number of the client or client(s), a description of the services rendered to the previous client(s), and the name of a responsible officer or employee of the firm who is knowledgeable about the services rendered to each client, if, in the 12 months preceding the date of the statement, services were rendered to RTD or any other client respecting the same subject matter of the RFP or directly relating to such subject matter. The client and contract number under which the services were rendered must also be included, if applicable. For financial interests, the statement must include the nature and extent of the interest and any entity or entities involved in the financial relationship. For these and any other interests, enough information must be provided to allow a meaningful evaluation of the potential effect of the interest on the performance of the Contract.

(5) A statement that no actual or potential conflict of interest or unfair competitive advantage exists with respect to the Work to be provided in connection with the Contract or that any actual or potential conflict of interest or unfair competitive advantage that does or may exist with respect to the Contract or related to the Contract has been communicated as part of the statement required by section (c).

(d) Failure of a firm to provide the required statement may result in the firm being determined ineligible for award. Misrepresentation or failure to report any fact may result in the assessment of penalties associated with false statements or such other provisions provided for by law or regulation.

ORGANIZATIONAL CONFLICT OF INTEREST CERTIFICATION

The proposer ❑ is ❑ is not aware of any information bearing on the existence of any potential organizational conflict of interest as described in the Disclosure Requirements on the previous page.

If the proposer is aware of information bearing on whether a potential conflict may exist, the proposer shall provide a disclosure statement describing this information as described in the Disclosure Requirements on the previous page.

Signature _____

Title _____

Date _____

Form W-9 Taxpayer Identification Number Request (Use this form to obtain TIN for payments of interest, dividends, or Form 1099-B gross proceeds)

To: _____ **Account:** _____

Please complete the following information. We are required by law to obtain this information from you when making a reportable payment to you, and because the payment is reportable on an information return to the IRS, you are required by law to provide your correct Social Security Number or Employer Identification Number to us. If you do not provide us with this information, your payments may be subject to 30% federal income tax backup withholding (29% after December 31, 2003). Also, if you do not provide us with this information, you may be subject to a $50 penalty imposed by the Internal Revenue Service under section 6723.

Federal law on backup withholding preempts any state or local law remedies, such as any right to a mechanic's lien. If you do not furnish a valid TIN, or if you are subject to backup withholding, the payer is required to withhold 30% of its payment to you (29% after December 31, 2003). Backup withholding is not a failure to pay you. It is an advance tax payment. You should report all backup withholding as a credit for taxes paid on your federal income tax return.

Use this form only if you are a U.S. person (including U.S. resident alien). If you are a foreign person, use the appropriate Form W-8.

Instructions:
1. Complete Part 1 by completing the one row of boxes that corresponds to your tax status.
2. Complete Part 2 if you are exempt from Form 1099 reporting.
3. Complete Part 3 by filling in all lines.
4. Return this completed form to us in the enclosed envelope.

Part 1 - Tax Status: *(complete only one row of boxes)*

Individuals: *(Fill out this row.)*

Individual Name: (First name, middle initial, last name)	Individual's Social Security Number
_____ _____ _____	___ ___ ___ — ___ ___ — ___ ___ ___ ___

A sole proprietorship may have a "doing business as" trade name, but the legal name is the name of the business owner.

Sole Proprietor (or an LLC with one owner): *(Fill out this row.)*

Business Owner's Name: (REQUIRED)	Business Owner's Social Security Number	Business or Trade Name (OPTIONAL)
_____ _____ (First name) (Middle Initial) _____ (Last name)	___ ___ ___ ___ ___ ___ ___ ___ ___ Or Employer ID Number ___ ___ ___ ___ ___ ___ ___ ___ ___	_____ _____

Partnership (or an LLC with multiple owners): *(Fill out this row.)*

Name of Partnership:	Partnership's Employer Identification Number	Partnership's Name on IRS records *(see IRS mailing label)*
_____ _____	___ ___ — ___ ___ ___ ___ ___ ___ ___	_____ _____

A corporation may use an abbreviated name or its initials, but its legal name is the name on the articles of incorporation.

Corporation, or Tax Exempt Entity *(Fill out this row.)*

Name of Corporation or Entity:	Employer Identification Number
_____ _____	___ ___ — ___ ___ ___ ___ ___ ___ ___

Part 2 - Exemption: If exempt from reporting, check your qualifying exemption reason below:

- ☐ Corporation — Note that there is no corporate exemption for medical and healthcare payments or payments for legal services.
- ☐ Tax Exempt Entity under 501(a) (includes 501(c)(3), or IRA
- ☐ The United States or any of its agencies or instrumentalities
- ☐ A state, the District of Columbia, a possession of the United States, or any of their political subdivisions or agencies
- ☐ A foreign government or any of its political subdivisions or an international organization in which the United States participates under a treaty or Act of Congress

Part 3 - Certification: Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), **and**
2. I am not subject to backup withholding because: **(a)** I am exempt from backup withholding, or **(b)** I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or **(c)** the IRS has notified me that I am no longer subject to backup withholding **and**
3. I am a U.S. person (including a U.S. resident alien).

Certification Instructions - You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return.

Person completing this form: _____

Signature: _____ Date: _____ Phone: (_____) _____

Address: _____ City: _____ State: _____ ZIP: _____

PART 3

STATEMENT OF WORK

We make lives better
through connections.

Statement of Work

RTD Website Redesign

Version: V1.0

November 16, 2022

Regional Transportation District
1660 Blake Street, Denver CO 80202

Statement of Work

Table of Contents

Statement of Work

Statement of Work

Executive Summary

The Regional Transportation District's (RTD) Digital Marketing department seeks a qualified contractor to implement a redesign of the public-facing website (rtd-denver.com). A competitive solution will propose a new Content Management System (CMS), as well as offer enhancements to the layout and streamline the process for RTD personnel to update and management content.

RTD seeks a Request for Proposal (RFP) from qualified contractors to deliver an end-to-end, full-service digital web experience for our customers.

Project Description

Scope of the Project

A. Current-State

- RTD-Denver.com has an average of 700,000 users and 1.5 million sessions per month.
- The current site utilizes about 350 pages.
- The Denver metro area public utilizes the site to find the latest information on bus and train fares, schedules, routes, trip information and much more.
- The underlying Content Management System currently in place is Drupal and hosted in the Acquia cloud environment. This solution has been in place for four years and requires unsustainable levels of maintenance from RTD's technology department.
- Stored content on the site is difficult to locate, retrieve and update for site administrators.
- Some content updates rely on developer expertise and cannot be easily implemented by non-technical business users. Drupal development requires unique expertise which is challenging and expensive to find.
- The current CMS includes outdated templates that could use a more modern design aesthetic.

B. Future-State

- A modern, mobile-first web design that enhances the users' digital experience.
- Updated CMS that allows for seamless content generation and editing.
- An updated look and feel that incorporates RTD's existing brand elements.
- An innovative platform that drives adoption and increases utilization from RTD's internal and external customers.

C. Goals and Objectives

- Maximize ease-of-use for web design and content management
- Lower existing and ongoing design and support costs
- Utilize a larger pool of resource expertise
- Implement a more responsive website, including faster page loading and mobile-first designs.

Statement of Work

- Provide an environment that is easier for developers to work in and accommodates changes in technical advancements.
- Provide a solution where the CMS decouples the presentation layer from the applications/data layer in the back end (headless CMS platform)
- Implement a secure environment
- Deploy seamless patching and updating
- Provide responsiveness across all platforms
- Easier content updates, redesign, and workflow
- Easier integration with third-party applications
- Responsive 24/7 customer support
- Improved return on investment (ROI) through time savings on updates and reduction in support costs for development hours.

Location

While RTD anticipates most of the work to be performed remotely, competitive bids may propose some onsite sessions, particularly for stakeholder interviews and gathering end-user requirements. When onsite, contractor can expect to work at or near the following RTD office location:

1660 Blake Street
Denver, CO 80202

Period of Performance

The work will initiate once a contractor has been selected and the contract is fully executed. The estimated duration for design and implementation is roughly 6-9 months but is dependent on the vendor estimates. Support and maintenance are expected to be needed for five years.

Roles and Responsibilities

Vendor Responsibilities:

- Conduct end-user interviews
- Conduct stakeholder interviews
- Gather functional requirements
- Determine technical dependencies, based on RTD's existing infrastructure
- Perform competitive analysis within the transportation industry
- Lead a branding workshop with key stakeholders
- Explore conceptual design options and iterate based on stakeholder feedback
- Build prototype
- Create a style guide
- Lead development effort

Statement of Work

RTD Responsibilities:

- Form a project team to work directly with the vendor
- Assign a project manager to coordinate work across all teams, schedule and lead status meetings and generate status reports per RTD IT PMO standards
- Participate in end-user and stakeholder interviews
- Facilitate end-user testing and gather feedback on prototypes
- Make decisions on design options
- Provide development resources to work alongside vendor
- Define go-live and ongoing support needs

Project Requirements

The project requirements that follow in this SOW are also documented in the Compliance Matrix. Please complete and return Attachment C – Compliance Matrix with your proposal.

Warranty information is documented in the Supplemental Technology Terms and Conditions.

Business Requirements

Business Requirement ID	Business Requirement Name	Description
REQ-1	Stakeholder Engagement	Contractor shall engage the various stakeholder groups (provided by RTD) to determine end-user business needs.

Functional Requirements

Functional Requirement ID	Functional Requirement Name	Description
REQ-2	eAccessibility	Initial design shall consider common web accessibility (eAccessibility) practices that allow for easy site navigation for users with disabilities and consider socio-economic restrictions to bandwidth and speed. Site design shall adhere to Web Content Accessibility Guidelines (WCAG) version 2.1 recommendations. Website implementation deliverables shall utilize Progressive Enhancement (PE), Landmark Elements for assistive technology, Semantic HTML, accessible defaults, accessible routing, and include an accessibility statement.
REQ-3	CMS Browser Compatibility	CMS site administration must be accessible from any modern internet browser.
REQ-4	Content Repository/Archiving	Previously published content, images and associated data shall be accessible to administrators of the site with minimal effort required for retrieving (i.e., keyword search). Additionally, historical page revisions shall be accessible to site administrators indefinitely via the CMS.
REQ-5	Document Updates	RTD requires easy-to-update documents that are modified with new content frequently. This includes, but is not limited to, the Board of Directors subpage (https://www.rtd-denver.com/board-of-directors), financial data (https://www.rtd-denver.com/financials-investors#financial-documents) and the News Stop section (https://www.rtd-denver.com/news-stop)

Statement of Work

Functional Requirement ID	Functional Requirement Name	Description
REQ-6	Content Owner Roles	RTD content owners responsible for applicable site subpages must be able to operationally manage content for their specific pages of the website (i.e., a news stop https://www.rtd-denver.com/news-stop)
REQ-7	Optimal Performance Measures	See Appendix A for a list of performative metrics that RTD requires for the future website.
REQ-8	Queued Content Updates	The preferred solution shall allow for the ability to preschedule content updates or to set a regular schedule (i.e., weekly) for automated changes. A date picker feature shall be incorporated for pre-loading and scheduling content to go-live at a future scheduled time and date.
REQ-9	Real-time content preview	The preferred solution would allow RTD content managers to preview changes before publishing them to the site.
REQ-10	Responsive Site Loading	The solution must provide responsive site loading, including page speed. Contractor shall provide evidence that solution is built for optimal performance.
REQ-11	Content Templates and Scalability	Solution shall allow for rapid creation of new content (i.e., new pages). Contractor shall collaborate with RTD stakeholders to establish a scalable content strategy and repeatable workflow. Solution shall have the option to drag and drop content and images once templates and styles are established.
REQ-12	Custom User Roles	The solution must allow for provisioning custom user roles for ease in managing specific content or working in the code base.
REQ-13	User-Centric	The redesigned public website (rtd-denver.com) shall focus on customers' transit and other needs and interactions and shall include such elements as enhanced search functionality and accurate and easy-to-use website navigation layout. End-users shall have easy access to up-to-date information, trip plans, schedules, new routes, etc.
REQ-14	Versioning	Solution shall allow for the ability to rollback current page builds to previous versions for production.
REQ-15	Web Browser Compatibility	Site will work seamlessly across all major web browsers.
REQ-16	Language Translations	Solution must support integrating a translation/localization option to allow site content to be submitted and translated into English, Spanish and (potentially) Simplified Chinese languages.

Technical Requirements

Technical Requirement ID	Technical Requirement Name	Description
REQ-17	Codebase Rewrite	The contractor, along with RTD's front-end developers, shall rewrite RTD's existing codebase for the existing 300-page marketing website (HTML/CSS/Javascript/PHP and Drupal's Drush) to work with the future solution that will continue to be housed in RTD's instance of GitHub. The new codebase shall incorporate modern front-end languages, e.g., JS, React, HTML, JSX, CSS
REQ-18	CMS/API Delivery	RTD content that is housed in the headless CMS will have the ability to be delivered via Application Programming Interface (APIs) for seamless display across various desktop, tablet and mobile devices.
REQ-19	CMS Hosting/Content Infrastructure	CMS and hosting of associated content shall be cloud-based and utilize microservices architecture. The content infrastructure shall allow for cross-collaboration and for developers to work in parallel as a team utilizing an Agile framework. Content infrastructure shall allow ease of reusability for content creation.
REQ-20	Decoupled Solution	The solution shall be a decoupled application utilizing JAMstack architecture with separate front and back ends that allow content edits and development work to occur asynchronously.
REQ-21	Github	A competitive solution shall provide seamless integration with GitHub's software and associated version control tool Git.

Statement of Work

Technical Requirement ID	Technical Requirement Name	Description
REQ-22	React and JAMstack architecture	A completive solution shall utilize a React and Javascript, APIs, and Markup (JAMstack) framework to provide the website experience.
REQ-23	Cloudfare integration	Solution shall be compatible with Cloudfare (RTD's current middle tier solution).
REQ-24	URL Redirection	Solution shall uphold all URL redirects that are in place for the current website.
REQ-25	Next Ride Application Integration	The new site shall incorporate RTD's recently built Next Ride application (https://beta.rtd-denver.com/) and contractor shall ensure it appears to end-users as part of the same site (look and feel, URL). Next Ride is built in Next.JS using React with the Chakra UI component library.
REQ-26	CMS Browser Extension	The recommended CMS solution shall allow for Chrome or similar extension to be used by content owners of specific pages of the site to edit and deploy content.
REQ-27	API Endpoints	The solution shall use all API endpoints existing on the current site (to be shared by RTD) in the development of the new website.
REQ-28	Analytics Platform Integration	Vendor shall integrate solution with RTD's existing analytics platforms Google Analytics 4 (GA4) and Google Tag Manager (GTM).
REQ-29	Existing Application Lookup Integration	Contractor shall develop a strategy and migrate existing lookup applications, including but not limited to: RTD's License Plate Lookup, Access-A-Ride, Board of Directors District Lookup, and Flex Ride service area.

Design Requirements

Design Requirement ID	Design Requirement Name	Description
REQ-30	Component libraries	Solution shall create reusable components to be utilized by RTD content creators throughout the site (i.e., updating a local fare token in one section of the site automatically updates fare postings throughout the site).
REQ-31	Design Systems	The collection of tools, platforms, applications and software that comprise the new technology stack shall be complementary of one another.
REQ-32	Developer Experience (DX)	The solution shall provide easy maintainability and debuggability, hot reloading of content, declarative rendering, componentization, declarative data queries, asset pipelines, Cascading Style Sheets (CSS) extensions, modern JS syntax and require a low level of effort for developers.
REQ-33	RTD Brand Standards	Redesign shall match RTD brand standards located at https://www.rtd-denver.com/brand-elements, while proposing guideline enhancements that visually connect with our audience.
REQ-34	Mobile-First Design	The site shall be designed to be viewed on mobile devices first, while also maintaining best-in-class design and functionality on laptops and desktops. Site shall work seamlessly across modern browsers on widely used smartphones, tablets and associated Operating Systems (OS).
REQ-35	Scope of Design Services	Design services shall include a path from initial concepts to functional prototypes.
REQ-36	Search Engine Optimization	The solution shall incorporate web design practices and integrations that align with industry-leading search engine optimization (SEO).
REQ-37	Usability	Product must be easy to use for RTD internal users who do not have technical expertise
REQ-38	Notification Banner	Solution shall include notification banner options on the site homepage for displaying messages to website visitors. Additionally, RTD needs the ability to display systemwide notifications with varying colors, depending on the message type. For example, success (green), information (blue), warning (orange), error (red), disabled and compact (grey).
REQ-39	Form Builder	Solution shall allow for the use of a form builder to pass information to RTD's Salesforce backend solution.

Design Requirement ID	Design Requirement Name	Description
REQ-40	Image Size Editing	The CMS shall allow for direct editing of image sizes to be displayed on landing pages within the CMS.
REQ-41	Reusable UI Components	Solution shall provide Image Component and Image Optimization using Next.js
REQ-42	Template Options	Contractor shall deliver multiple template options to differentiate page layout, structure, and design throughout the site.

Project Management Requirements

PM Requirement ID	PM Requirement Name	Description
REQ-43	Kick-off Meeting	A Project Kickoff Meeting, coordinated with the RTD Project Manager, shall be scheduled within seven (7) days after Notice to Proceed (NTP) and conducted within twenty-one (21) days. The Project Kickoff Meeting will be conducted by the Contractor and the RTD Project Manager at RTD offices, through Microsoft Teams, or other high-quality teleconferencing approach.
REQ-44	Project Meetings	The RTD Project Manager shall schedule and facilitate Progress Meetings held between the Contractor and the RTD on a weekly or every other week basis, as deemed necessary by the RTD, for the purpose of reviewing progress, coordinating activities, and other project activities that cannot be resolved by correspondence. The timing of these meetings shall be conducted at the RTD's sole discretion, based on the nature of the current project activities. These meetings may be at RTD offices, through Microsoft Teams, or other high-quality teleconferencing approach.
REQ-45	Project Meeting Agendas	Agendas for the Progress Meetings will be prepared by the Contractor and may include any topics that the Contractor's Project Manager determines to be relevant to the project. The Contractor shall insure those persons knowledgeable in the topics to be discussed, including subcontractors, subject matter experts, and/or technical representatives, are present at all necessary meetings. Agendas will be submitted at least two (2) business days prior to the meeting.
REQ-46	Meeting Summaries	Meeting summaries shall be taken at all meetings. Summaries shall include a summary of all topics discussed, a listing of all understandings and agreements reached, and an updated Action Item List (AIL). Unless otherwise agreed, the Contractor shall be responsible for taking all meeting summaries. The format for the meeting summaries shall be developed based on input from the RTD.
REQ-47	Meeting Summaries	The meeting summaries shall be distributed to all attendees for review within three (3) business days from the end of the meeting.
REQ-48	Action Item List	During meetings, action items will be identified, with each action item assigned to an individual for disposition by a pre-determined response date. These action items shall be maintained and updated throughout the project by the Contractor, in an Action Item List (AIL). The AIL format will be mutually agreed upon by the Contractor and the RTD.
REQ-49	Issue Tracking systems	The Contractor shall provide RTD key personnel access to any issue tracking system used by the Contractor for Sprint planning during the project. The Contractor will provide no less than monthly a status report of all tickets.
REQ-50	Monthly Status Report	Contractor shall provide to the RTD PM a status report monthly highlighting key accomplishments, risks, issues, and milestones/deliverables updates.
REQ-51	Invoice Documentation	The Contractor shall keep and maintain reasonably complete and reliably detailed records of milestones achieved in performing the Contract, including records of productivity to identify basis for payment, sufficient to evaluate the accuracy, completeness, and currency of the costs or prices.
REQ-52	Project Schedule	Within thirty (30) days after Notice to Proceed (NTP), the Contractor shall furnish, to the RTD for the RTD's approval, a detailed Project Schedule. The detailed

Statement of Work

PM Requirement ID	PM Requirement Name	Description
		Project Schedule shall be based on critical-path-method and constructed using Microsoft Project or RTD approved substitute.
REQ-53	Project Schedule	The detailed Project schedule shall show start and completion of the work with dependencies for each activity and shall be properly ordered and sequenced. It shall identify all major work tasks including critical events of design, procurement, delivery schedule, installation, testing, and integration, and shall identify interface activities, subcontractor contributions and submittals, RTD inspections, tests, and approvals as may be required by this document, additional details shall be provided, such as: · A clear description of the activity, including its location · The duration expressed in full working days · A responsibility for work denoting the Contractor, a subcontractor, RTD, or entity performing the activity · The quantity of material, in units · Type of equipment needed (if significant or unusual) · The integer percent complete representing the installed progress · The actual start and finish dates when applicable Requirements and events which impose limitations, as well as dates and milestones which constrain the time, shall be clearly identified.
REQ-54	Personnel	All personnel assigned by the Contractor must display appropriate identification while on RTD property and must adhere to all RTD Rules and Regulations.
REQ-55	Project Schedule Updates	The Contractor shall be required to submit project schedule updates on at least a monthly basis. More frequent near-term schedule updates may be required, if deemed advantageous by the RTD for monitoring the progress of specific phases of the project.
REQ-56	Project Communications	Within thirty (30) days of Notice to proceed (NTP), the Contractor shall provide a RACI along with Contractor's escalation procedure, including contact names and information for each level of escalation.
REQ-57	Project Communications	The Contractor shall promptly notify the RTD PM of any problems or difficulties that may affect the timely or effective completion of the project or any scheduled deliverables.
REQ-58	Project Communications	The Contractor shall coordinate activities with RTD PM regarding affected RTD business units and personnel, and with external individuals and organizations.
REQ-59	Subject Matter Experts	The Contractor shall make all subject matter experts available - when required or requested.

QA Requirements

QA Requirement ID	QA Requirement Name	Description
REQ-60	Quality Assurance	The Contractor shall plan, establish, and maintain a Quality Assurance (QA) program. The Contractor's QA program shall be imposed upon all entities within the Contractor's organization and on all subcontractors whenever contract work is performed.
REQ-61	Quality Assurance	A QA Program Plan shall be submitted for review within 30 days of Notice to Proceed (NTP). The QA Program Plan shall describe the methods for planning, implementing, and maintaining quality, schedules, and cost. The QA Program Plan shall contain a company policy statement that clearly defines the authority and responsibilities of QA personnel.

Statement of Work

Training Requirements

Training Requirement ID	Training Requirement Name	Description
REQ-62	User Role Training	Contractor shall provide training for all hands-on roles for maintaining the platform utilizing RTD's implementation, where practical.

Support and Maintenance Requirements

Support and Maintenance Requirement ID	Support and Maintenance Requirement Name	Description
REQ-63	CMS Support & Maintenance	Contractor shall provide on-demand support as requested from RTD based on a retainer work order contract. RTD resources must be able to manage and support normal operations after website go-live. Contractor to include a quote in the RFP response for an initial 1, 000 support hours retainer, to include the hourly bill rate. RTD anticipated support needs may include future custom development, assistance with large system upgrades and technical troubleshooting.

Documentation Requirements

Documentation Requirement ID	Documentation Requirement Name	Description
REQ-64	Documentation	All documentation shall be in English, shall utilize Imperial measurements, and shall be submitted directly to RTD electronically in the following formats, as applicable: MS Office formats (DOC, XLS, PPT, VSD) Adobe PDF (searchable) Scanned documents consisting of signatures, etc. may be approved for submittal.
REQ-65	Documentation (Manuals)	The vendor shall provide written detailed system operation, administration, configuration, architecture, and maintenance manuals to RTD. Manuals shall be complete, accurate, and up-to-date, and shall contain only information that pertains to the system(s) installed.
REQ-66	Documentation	All pages of the documentation shall carry a title, version number and issue date. All manuals shall contain a complete subject index.
REQ-67	Documentation	Documentation shall require re-issuance if any change or modification is made to the system proposed to be supplied. The Contractor may re-issue individual sheets or portions of the documentation that are affected by the change or modification. Each re-issuance or revision shall carry the same title as the original, with a change in version number and issue date.
REQ-68	Documentation	Approved documentation shall be a condition of final acceptance, and updated documentation will be required at any time the Contractor provides software or hardware upgrades. If the documentation as submitted is found to be unacceptable due to incompleteness or inaccurate information, the documentation shall be returned to the Contractor for corrective action and resubmitted for acceptance prior to the release of Final Acceptance payment.
REQ-69	Documentation	The Contractor shall provide Interface Control Document (ICD) and Entity Relationship Diagram (ERD) for all interfaces.
REQ-70	Collaboration Tools	The Contractor shall use RTD's Microsoft Team Site for document sharing/repository.
REQ-71	System Recovery Plan	The Contractor shall provide a system recovery plan detailing the procedures and timelines in ensuring system operability is restored within 24 hours.

Documentation Requirement ID	Documentation Requirement Name	Description
REQ-72	System Implementation Plan	The Contractor shall develop a System Implementation Plan (SIP) no less than 60 days prior to start of system implementation. The SIP describes how the System will be installed, deployed and transitioned into an operational System. The SIP will contain an overview of the System, a brief description of the major tasks involved in the implementation, assumptions, constraints, risks, the overall resources needed to support the implementation effort (e.g., hardware, software, facilities, materials, and personnel), and the cutover plan to transition to the new System with minimal adverse impact to RTD's operations. The overall sequence and site-specific implementation specifications will also be documented. The SIP must be approved by RTD prior to its implementation.

Personnel Requirements

Personnel Requirement ID	Documentation Requirement Name	Description
REQ-73	Cross-Collaboration	RTD developers shall work with contractor developers in sprints throughout the project to understand how to manage and work with the new code repositories and CMS.
REQ-74	Joint Design and Development Collaboration	Contractor shall collaborate with RTD designers and developers on the new site design.

Product and Service Requirements

Product and Service Requirement ID	Documentation Requirement Name	Description
REQ-75	Migrate RTD Legacy Content Repository	The current website contains numerous images, PDFs, videos and files stored on the existing CMS. Contractor shall facilitate migration of the legacy content onto the new CMS.

Security Requirements

Security Requirement ID	Documentation Requirement Name	Description
REQ-76	Minimum Viable Use	The product(s) created and purchased for this solution shall have a minimum viable use of three (3) years from the date of purchase. Products that are end of life or scheduled for sunset within three years of the date of purchase are ineligible. Should the product purchase be part of an overarching service contract that includes the ongoing purchase, installation, and maintenance of commercially available equipment over a fixed term, purchased products must be replaced when they reach end-of-life status.
REQ-77	Patches and Upgrades	Should the product include software or firmware components, to maintain the currency, supportability, and security of the product software or firmware, the product shall be accompanied by a maintenance or licensing agreement that shall, at minimum, include patches for security and bug fixes (including roll up packages for updates, e.g., service packs) and incremental version upgrades for no less than three consecutive years from the installation date.

Statement of Work

Security Requirement ID	Documentation Requirement Name	Description
REQ-78	Implementation Guide	The product shall be accompanied by clear and unambiguous written instructions (e.g., a manual or product implementation guide) on how to set security features for the product. At minimum, the instructions shall address access control features, including changing of default user IDs and passwords post-installation and managing encryption keys (as applicable). For networked products, the instructions shall additionally include a list of the minimum necessary services, ports and protocols required to facilitate communication between this product and others (e.g., a database server).
REQ-79	Responsible Sourcing	Products with Department of Homeland Security directives against purchase or that are sold or manufactured by companies on the Department of Labor Office of Federal Contract Compliance Programs Debarred Companies list are ineligible. Additionally, to the extent that it is possible to provide, the Contractor shall provide RTD with additional information about the manufacture or acquisition of safety or security sensitive products to ensure they are responsibly sourced and reduce the risk of embedded threats and vulnerabilities.
REQ-80	Logging	The product shall support or facilitate logging and forwarding of application security events for operational failure, security incident, and security monitoring purposes.
REQ-81	Access Control and Authority	The product shall contain features that allow administrators to control user and system access to functions, features, or system components a need-to-know basis. The product must be able to operate with user level authority and must not require that a user be logged in as an administrator to operate properly. Users and administrators of the product must be able to change and otherwise manage their credentials (for example, establish a password and perform password resets).
REQ-82	Data Security	Products that are intended for the storage, processing, or transfer of sensitive data shall support strong encryption at rest. Products that communicate over the Internet, for example, for authentication, maintenance purposes, or remote management, shall use unbroken encrypted communication methods. Products that store sensitive data shall tolerate and/or enforce purging data that RTD determines no longer has a business need to be retained.
REQ-83	Proof of Concept	Proof of concept systems and environments shall be physically and logically separate from RTD production systems and shall not require the use of any production RTD data.
REQ-84	Exceptions	Should a product be necessary to fulfill the scope of services under the Agreement, yet incapable of conforming to some or all the aforementioned requirements, the Contractor shall identify the non-conforming product to RTD and the specific requirements that are not met to afford RTD the opportunity to understand the risks to RTD's operations. The Contractor shall additionally explore and present alternatives, including but not limited to use of a different product, configuration options, or other risk mitigation measures, and present those opportunities to mitigate risk (if any) to RTD. The Contractor shall not install a non-conforming product without RTD's written approval.
REQ-85	Control Activities	At RTD's request, Contractor shall provide RTD the opportunity to review the design and execution of the control activities performed by the Contractor as relates to the support and security of RTD's operations and the data, systems, networks, or facilities that are relevant to providing services to RTD (as applicable to the scope of services).
REQ-86	Disaster Recovery and Business Continuity	Contractor shall maintain and implement a disaster recovery plan to ensure continuity of the services provided to RTD pursuant to this Agreement and the recovery of any data or functionality lost due to operator error, system error or other unforeseen circumstances. Upon written request, Contractor shall provide RTD with a copy of its current disaster recovery plan and all updates to these plans during the term of this Agreement. In addition, Contractor shall maintain and implement a business continuity plan for the term of this Agreement. Upon RTD's written request, Contractor will issue to RTD a summary statement on the design of the business continuity management framework. The Business Continuity Plan is

Security Requirement ID	Documentation Requirement Name	Description
		confidential, and Contractor will not provide actual plans, nor will it allow customers to participate in business continuity activities.
REQ-87	Multi-Tenancy	Should a multi-tenancy architecture be used, Contractor shall implement and maintain access controls to adequately separate the functions of each environment such that actions taken in or for another customer do not affect the security of RTD's data or operations on the same architecture.
REQ-88	SOC 2 Type 2 Report	Fourteen calendar days after receipt of the NTP, Contractor shall provide to RTD their most recent Service Organization Control (SOC) 2 Type 2 report pertaining to the scope of services provided to RTD. Thereafter, for the term of this Agreement, the Contractor shall provide an updated SOC 2 Type 2 report to RTD on an annual basis. If Contractor fails to provide an updated SOC 2 Type 2 report, then Contractor will notify RTD in writing of a date when the SOC 2 Type 2 report will be made available to RTD, except that the updated SOC 2 Type 2 report must be made available to RTD no later than 18 months after the last report was produced. If Contractor's SOC 2 Type 2 report is qualified, then Contractor will provide a written Plan of Actions and Milestones to notify RTD of what actions they are taking to correct any findings and the expected resolution date for those corrections. Should a SOC 2 Type 2 not be performed or available, an alternative third-party control audit report may be acceptable to RTD with prior notice, sufficiency of criteria review, and approval from RTD.
REQ-89	Risk Assessment	Contractor shall perform a risk assessment prior to any major system change or installation that impacts the storage, collection, transmission or processing of RTD Data, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting RTD Data, or changes in security controls related to RTD Data. Identified risks and mitigation plans must be reviewed with RTD prior to change implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.
REQ-90	Vulnerability Testing	Contractor shall perform a risk assessment prior to any major system change or installation that impacts the storage, collection, transmission or processing of RTD Data, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting RTD Data, or changes in security controls related to RTD Data. Identified risks and mitigation plans must be reviewed with RTD prior to change implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.
REQ-91	Recovery Point Objective (RPO)	Data backups shall occur no less frequently than once every (12) hours.
REQ-92	Recovery Time Objective (RTO)	The amount of downtime for a system outage shall not exceed (60) minutes.
REQ-93	Single Sign-On (SSO)	Software shall be capable of SSO integration with Microsoft Azure for developer access.
REQ-94	Multi-Factor Authentication (MFA)	Software shall be compatible with widely available Two-Factor Authentication (2FA) technology.
REQ-95	Transport Layer Security (TLS) Encryption	Solution shall be capable of encryption in transit with TLS version 1.2 or higher.
REQ-96	Certificate Authority (CA)	Website security certificates shall be managed and maintained by the Contractor.

Statement of Work

Product Requirements

Product Requirement ID	Documentation Requirement Name	Description
REQ-97	Content Management System (CMS)	Contractor shall propose a Content Management System solution to replace RTD's current Drupal-hosted CMS with a modern, easier-to-use platform. Contractor's proposed solution must be fully capable of supporting React-based websites.
REQ-98	Headless Content Management System (CMS)	Contractor shall propose a headless CMS solution where the content repository "body" is separated or decoupled from the presentation layer "head."
REQ-99	Content Migration	The Contractor solution must have the functional ability to migrate content from the current CMS to the future solution. Contractor shall provide resources to implement content migration from the legacy RTD website to the new site based on total amount of content (RTD's current site has approximately 350+ pages).
REQ-100	Design Deliverables	Contractor shall provide documentation related to managing and updating the site including but not limited to: landing page style guide, taxonomies, necessary resources to edit the site, user flow diagrams, brainstorming notes, etc. Page architecture and elements will follow UX principles in displaying content clearly, prominently displaying call to actions (CTAs), headings, etc.
REQ-101	User-Friendly Content Management System	The solution must use a CMS that does not require coding or specialized skill sets to make changes to content.
REQ-102	Contractor References (sites)	Contractor will provide (3) examples of site designs of similar size and scope to RTD's current site.
REQ-103	Content Delivery Network (CDN)	Vendor, with RTD agreement, shall recommend a CDN to implement.

Performance Measures

Vendor Evaluation Criteria

Criteria	Weight (%)
A. Cost: including specificity of the Pricing Form and inclusion of all elements of the compliance matrix in the costs identified.	**30%**
B. Experience of the company and key personnel regarding the business needs of RTD as defined in the Scope of Work.	**20%**
C. Technical and functional specifications of the website, including security and data management, implementation strategy, and timeline for completion.	**25%**
D. Design proposal explaining the research and design phases and approach, and special recommendations for RTD.	**25%**
TOTAL	**100%**

Statement of Work

Project Milestones

The following deliverables are to be provided by the contractor:

Deliverables
Project Plan
Current-State Review (website content, processes, workflow)
Stakeholder interviews
Initial Design (low fidelity wireframes)
Customer feedback, design iterations
Prototypes
Architecture and Technical planning
Detailed Design (high fidelity wireframes)
Content Migration plan
Cutover and Deployment
Training Manuals
Style Guide
Transition to Support

Glossary

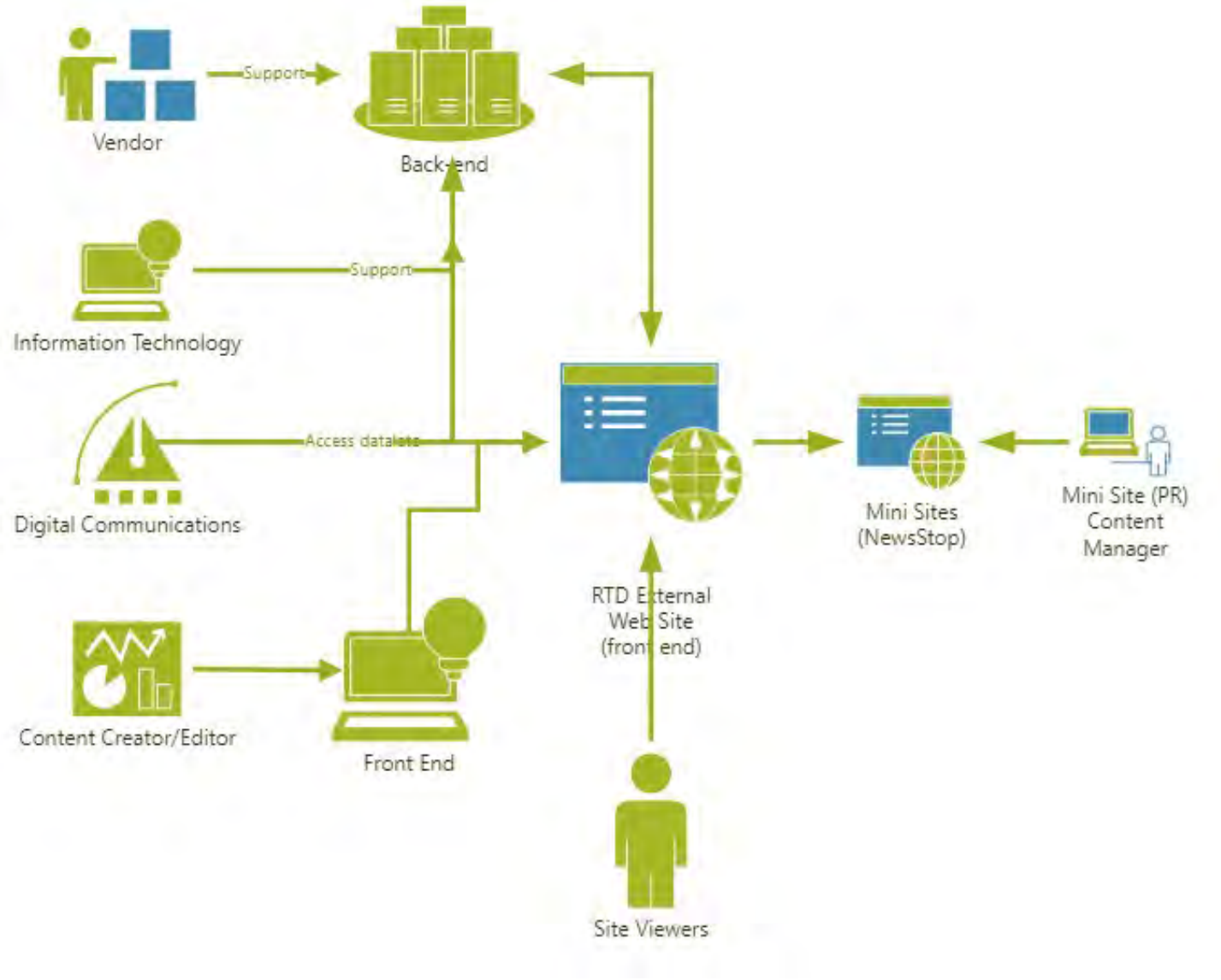
Name	Alias	Description
Content		Refers to the textual, aural, or visual content published on a website. Content means any creative element, for example, text, applications, images, archived e-mail messages, data, e-services, audio and video files, and so on. Web content is the key behind traffic generation to websites.
Content Management System		A content management system is a software application that can be used to manage the creation and modification of digital content. CMSs are typically used for enterprise content management and web content management.
Decouple		Decoupled, or decoupling, is a state of an IT environment in which two or more systems somehow work or are connected without being directly connected. It is a type of IT operational environment where systems, elements or components have none or very little knowledge about the other components.
Drupal		A free and open-source web content management framework written in PHP and distributed under the GNU General Public License.[4][6][7] Drupal provides a back-end framework for

Statement of Work

Name	Alias	Description
		websites worldwide. Systems also use Drupal for knowledge management and for business collaboration.
Future Proof		A buzzword that describes a product, service or technological system that will not need to be significantly updated as technology advances.
Page Speed		Less than 3 seconds is the recommended page load time for websites on both mobile and desktop devices.
Scalable		The characteristic of a system, model, or function that describes its capability to cope and perform well under an increased or expanding workload or scope.
Search Engine Optimization		The process of optimizing your website to get organic, or un-paid, traffic from the search engine results page. To do this, search engines will scan, or crawl, different websites to better understand what the site is about.
Site Loading		Ideal Website Load Time - 2 to 5 seconds. However, each second beyond 2 seconds results in greater bounce rates. In fact, 40% of polled internet users report abandoning a site if it takes longer than 3 seconds to load. Moreover, 47% of users expect desktop sites to load in 2 seconds or less.

Context Diagram

Statement of Work



Appendix A

Measurement Categories	Topics
Performance	Delivery Optimization, progressive image loading, responsive image loading, page caching, allow browsers to serve content locally, no extraneous code fetching
Developer Experience (DX)	maintainability and debuggability, hot reloading of content, declaritive rendering, componentization, declarative data queries, asset pipelines, CSS extensions, use of TypeScript
Governance	Secure, Access Control (CORS), environment variables, user authentication, design systems, component libraries
Accessibility	progressive enhancement, landmark elements are used, semantic HTML, accessible defaults, accessible routing, accessibility statement, WCAG 2.1 compliance
Documentation	tutorials and guides, sourcing data, incorporating CSS libraries, development guides, routing, testing, debugging, performance, adding search, adding analytics, adding authentication, adding SEO
Ecosystem	component ecosystem, themes ecosystem, integrations, hosting, paired programming, contributing section in documentation
PageSpeed Insights, Lighthouse	The top 3 most visited pages (including the homepage) should have scores for both mobile and desktop in the 90-100 range for Accessibility, Best Practices, SEO and 80-100 range for performance

CONTRACT 122DH059

Website Redesign

CONTRACT CONTENTS

CONTRACT AWARD and SIGNATURE PAGE

RTD Contract Number 122DH059

ISSUED BY	CONTRACTOR
Regional Transportation District 1660 Blake St. Denver, Colorado 80202 - 1399 Notices to: Ron Bibeau, Contract Administrator	[Name] [Address] [City, State, ZIP] Notices to: [CONTRACT REP NAME], Contract Representative

Invoices: Submit invoices as stated in Contract Section I, Statement of Contract Cost, Invoicing

Products/Services: Website Redesign

Contract Cost: [Inclusive of any fixed fee and cost detailed on Statement of Contract Cost]

Type: Firm Fixed Price (FFP)

Effective Date: Date of execution by RTD of this Contract Award and Signature Page

Period of Performance: Subject to the Termination provision of the Contract, performance shall commence as of the date specified in the notice to proceed or, if no date is specified, upon Contractor's receipt of notice to proceed, and shall continue for five (5) years. If mailed, receipt of the notice to proceed is presumed to be five days after mailing.

This Contract consists of: Contract Award and Signature Page; Section I – Statement of Contract Cost; Section II - Scope of Work (provided as Part 3 of RFP); Section III – Terms and Conditions, including exhibits; and Section IV – Attachments. These Contract Documents constitute the entire Contract between the parties.

Contractor's Agreement	Award
Contractor agrees to perform the Work identified above and on the continuation pages for the consideration stated herein and to otherwise perform according to the terms of the Contract. In executing this Contract, the Contractor warrants that it is familiar with the Scope of Work attached and that it is qualified to provide the associated level of effort required to successfully complete such tasks and that it can satisfactorily perform such tasks within the Contract Cost.	Regional Transportation District hereby accepts your offer to perform the Work identified above and on the continuation pages, for the consideration stated above, and in accordance with the terms and conditions of the Contract.
FOR By: _____ Name (print): _____ Title: _____ Date: _____	FOR THE REGIONAL TRANSPORTATION DISTRICT By: _____ Debra A. Johnson General Manager and CEO Date: _____ Approved as to legal form for the Regional Transportation District By: _____ Legal Counsel Name (print): _____ Date: _____

SECTION I STATEMENT OF CONTRACT COST

STATEMENT OF CONTRACT COST

For the satisfactory performance and completion of the Work, RTD will pay the Contractor compensation as set forth below. Capitalized terms shall have the meaning prescribed in the Contract, unless the context requires otherwise.

A. Term. Subject to the Termination provision of the Contract, performance shall commence as of the date specified in the notice to proceed or, if no date is specified, upon Contractor's receipt of notice to proceed, and shall continue for 5 years. If mailed, receipt of the notice to proceed is presumed to be five days after mailing.

B. Compensation.

1. This is a fixed-price Contract with a maximum price not to exceed [**$ TOTAL CONTRACT PRICE]**, within which price Contractor agrees to complete the Work as per the Contract Documents. Compensation for Work shall be on a fixed price per unit of supplies ordered and for installation of such equipment, if required, and/or on a fixed price per hour for services in accordance with the negotiated pricing schedule included with this Statement of Contract Cost. Payments shall be made in accordance with the payment milestone schedule included with this Statement of Contract Cost.

Payment Milestones	Percentage of Overall Contract
a) Design Completion	25%
b) Development of Website	50%
c) Final Delivery/Functional Site	25%

The Subscription and Service and Maintenance portions of the Contract shall be invoiced and paid Yearly – separate from the above components.

2. All prices, rates and costs shall be inclusive of all fees associated with the Contractor's efforts, including but not limited to salaries, benefits, expenses, overhead, administration, profits, and outside consultant fees. No hourly charges shall exceed any hourly rates identified in this Statement of Contract Cost or Contract amendment. Contractor shall not invoice separately for mileage, travel time, parking expenses or any other miscellaneous charges.

3. RTD shall not pay the Contractor for any Work performed or for any cost incurred by the Contractor or subcontractors prior to the Period of Performance, unless those costs are incurred pursuant to RTD written notice to proceed and the costs are directly related to deliverable items set forth in the Scope of Work. RTD shall not be required to pay any amount in excess of the Contract Cost, unless the Contractor has secured a written amendment to this Contract providing for such increase.

C. Discounts. If a prompt-payment discount is negotiated, its terms will be specifically identified in this Statement of Contract Cost. For purposes of earning such discount, payment shall be deemed tendered as of the date such payment is placed in the U.S. Mail.

D. Invoicing.

The Contractor shall submit invoices according to completion and acceptance by RTD of the attached payment milestones.

1. Invoices shall include:
   a) The Contractor's legal name;
   b) The Contract number;
   c) The Purchase Order number;
   d) The payment milestone number;
   e) Description of payment milestone;
   f) The total Contract Cost;
   g) The total amount due on the invoice, specifying amount of supplies and services, respectively, due under the invoice, and all documentation; and
   h) All other information specifically required by the Scope of Work.
2. Contractor shall submit the following with its invoices:
   a) A Progress Report detailing all Work accomplished during the reporting period. Progress Reports shall be in narrative form, brief and informal in content, but shall include:
      (i) A quantitative description detailing all Work performed and percentage of completion by phases of the Scope of Work and required deliverable items;
      (ii) Identification of any current or anticipated problems which may impede Contractor's performance and the proposed corrective action; and
      (iii) A brief discussion of the Work to be performed during the next reporting period.
3. Submit invoices to:

   AP.Department@RTD-Denver.com

E. Payment. Payment to the Contractor shall be made upon RTD's determination that all Work submitted for payment has been performed and all information and documentation required under the invoice and work order, if any, has been submitted. Payment will be made to the Contractor within 30 days after RTD approval of submitted invoices.

1. Prompt Payment of Subcontractors. The Contractor agrees that:
   a) It shall pay its subcontractor(s) any undisputed amounts for the satisfactory performance of their Work within seven days of the Contractor's receipt of payment from RTD for such Work;
   b) Within 30 days after a subcontractor's Work has been satisfactorily completed and accepted by RTD's Project Manager or by the Contractor, whichever is earlier, the Contractor shall make full payment to the subcontractor of any retainage the

Contractor has kept related to such subcontractor's Work, unless a claim is filed against the subcontractor related to such Work;

c) Failure to comply with the above may give RTD just cause to impose one or more of the following penalties, until the required payment(s) to the Contractor's subcontractor(s) is satisfied, unless RTD has given prior written approval to the Contractor for the delay or postponement of payment(s): (1) withhold payments to the Contractor; (2) assess sanctions against the Contractor; (3) assess the subcontractor's indirect or consequential damages against the Contractor; (4) disqualify the Contractor from future bidding on RTD contracts as non-responsible; (5) enforce the payment bond against the Contractor; (6) pay the subcontractor(s) directly and deduct this amount from any retainage owed to the Contractor; (7) provide notice of default to the Contractor, stating the potential for termination or suspension of the Contract, in whole or in part; (8) issue a stop-work order until the subcontractor(s) is paid, which order shall constitute an unauthorized delay under the Contract that could result in liquidated damages against the Contractor. Unless approved by RTD, the Contractor's failure to comply with this Section is a material breach of the Contract;

d) It shall ensure that tiered subcontractors comply with this Section and that they insert provisions (a) and (b) of this Section into all lower-tiered subcontractor agreements; and

SECTION III TERMS AND CONDITIONS

GENERAL TERMS AND CONDITIONS

TABLE OF CONTENTS

EXHIBITS TO TERMS AND CONDITIONS

ARTICLE 1. DEFINITIONS

Unless otherwise defined in this Contract, capitalized terms shall have the meanings ascribed to them. The following definitions shall apply throughout the Contract:

Contract. This agreement, specifically consisting of the documents described in "Documents Forming the Contract" and any amendments to the Contract.

Contractor. The individual, firm, company, corporation, partnership, or association entering into this Contract with RTD. The Contractor shall be identified on the Contract Award and Signature Page. Wherever used in this Contract, the term "Contractor" shall also refer to the Contractor's employees, agents, subcontractors, and any designated representative, whose authority to act on the Contractor's behalf shall be delegated in writing.

RTD. The Regional Transportation District, a political subdivision of the State of Colorado. Whenever used in this Contract, the terms "Regional Transportation District" or "RTD" shall include RTD's General Manager, subject to limitations of authority established by RTD's Board of Directors, and, if so designated, the Contract Administrator or Project Manager.

Work. The work and services to be performed by the Contractor for RTD's benefit pursuant to this Contract as detailed in the Scope of Work and other Contract Documents, including all administrative, deliverables, design, documentation, engineering, equipment, installation, labor, legal, management, manufacturing, materials, supervision, testing, verification, and any other duties and services, professional or otherwise, to be furnished and provided by the Contractor as required by the Contract, including all efforts necessary or appropriate to achieve final acceptance of the Work contemplated by the Contract.

ARTICLE 2. DOCUMENTS FORMING THE CONTRACT

This Contract consists of the following documents and any amendments (collectively, "Contract Documents"):

- Contract Award and Signature Page;
- Section I, Statement of Contract Cost;
- Section II, Scope of Work;
- Section III, Terms and Conditions, including Exhibits; and
- Section IV, Attachments.

ARTICLE 3. CONTRACT ORDER OF PRECEDENCE

In the event of inconsistency among any provisions of this Contract, the inconsistency shall be resolved by giving precedence in the following descending order:

1. Amendments to the Contract, if any;
2. Special Provisions/Alterations prescribed by Exhibit 3 to the Terms and Conditions, if any;

3. All other exhibits to the Terms and Conditions;
4. Contract Award and Signature Page;
5. Terms and Conditions that supplement the General Terms and Conditions, if any;
6. General Terms and Conditions;
7. Scope of Work and/or Specifications (also referred to as Technical Specifications);
8. Statement of Contract Cost; and
9. Attachments.

Unless expressly agreed by RTD in the form of a Special Provision/Alteration prescribed by Exhibit 3 or Contract amendment, any agreement, license, provision, or other document not listed above but made a part of this Contract shall be deemed an Attachment for purposes of determining Contract order of precedence.

ARTICLE 4. RTD CONTRACT ADMINISTRATION

A. **General Manager.** RTD's General Manager shall be identified by name on the Contract Award and Signature Page. The General Manager shall have the sole authority, subject to monetary limitations established by the Board of Directors, to enter into, amend or terminate this Contract, and these duties may not be delegated except by written instrument authorized by the General Manager or RTD's Board of Directors.

B. **Letter of Delegation.** RTD's General Manager may designate person(s) to act in his or her behalf in the general administration of this Contract. The General Manager's delegation of duties must be made in writing ("Letter of Delegation") with a copy delivered to the Contractor. Any General Manager Letter of Delegation shall include the extent of delegation of authority and any limitations on such authority. The General Manager may issue one or more Letters of Delegation and may at any time issue a new Letter of Delegation replacing the person(s) previously named.

C. **Contract Administrator.** The General Manager may designate a Contract Administrator, who shall be identified in a Letter of Delegation and on the Contract Award and Signature Page, to assist in the general administration of this Contract. Any such Letter of Delegation shall describe the extent of the Contract Administrator's duties, but, unless further express delegation from the General Manager is provided, the Contract Administrator does not have the authority to enter into, amend or terminate this Contract. In the Contract Documents and solicitation, the Contract Administrator may also be referred to as the Contracting Officer, Purchasing Agent, Buyer, or the like.

D. **Project Manager.** The General Manager may designate a Project Manager, who shall be identified in a Letter of Delegation, to administer the Work for RTD. Any such Letter of Delegation shall describe the extent of the Project Manager's duties, but, unless further express delegation from the General Manager is provided, the Project Manager does not have the authority to enter into, amend or terminate this Contract.

ARTICLE 5. EFFECTIVE DATE, PERIOD OF PERFORMANCE

A. Effective Date. The Effective Date of this Contract is the date of RTD's signature on the Contract Award and Signature Page. The Contract shall be effective until Contract closing. This Contract shall be considered closed after all Work has been accepted by RTD, RTD has received all necessary Closing Documents, and the Contractor has received final payment, provided however that certain terms and conditions shall, by their nature, survive closing of this Contract.

B. Period of Performance. Performance shall commence as of the date specified in the notice to proceed or, if no date is specified, upon Contractor's receipt of notice to proceed. The Period of Performance is specified on the Contract Award and Signature Page.

ARTICLE 6. OPTIONS

RTD shall have the option to extend this Contract in accordance with the option terms, if any, negotiated on the Statement of Contract Cost. RTD shall give notice to the Contractor at least 60 days prior to the expiration of the Contract if RTD intends to exercise the next option. The Contractor's receipt of preliminary notice does not commit RTD to exercise an option to extend. RTD may exercise the option provision more than once, but the total extension of performance under the Contract shall not exceed the total number of option terms negotiated. If RTD exercises the option to extend, the Contract shall be amended to include the option provisions.

ARTICLE 7. CONSIDERATION

A. In consideration of the Contractor's satisfactory performance of the Work in full compliance with the Contract, RTD shall pay the Contractor in accordance with the Statement of Contract Cost.

B. RTD shall not pay the Contractor for any Work performed prior to the Period of Performance.

C. RTD shall not be required to pay any amount in excess of the Contract Cost, unless the Contractor has secured a written amendment to this Contract providing for such increase.

ARTICLE 8. INVOICING AND PAYMENT

Invoicing and payment procedures are detailed in the Statement of Contract Cost.

ARTICLE 9. CONTRACT CLOSING PROCEDURES AND FINAL PAYMENT

A. Contract Closing Procedures. Upon Contractor's satisfactory performance of the Work in full compliance with this Contract, or upon termination of this Contract, whether for convenience or default, RTD shall provide the Contractor with the following Closing Documents: the Contractor's Release and the Contractor's Assignment of Refunds, Rebates, Credit and Other Awards.

B. Final Payment. Prior to final payment under the Contract, and as a condition precedent to final payment, the Contractor shall execute and deliver all Closing Documents to RTD.

ARTICLE 10. ACCESS TO RECORDS AND REPORTS

A. For a period of the longer of three years or such other time as required by another provision in this Contract following Contract closing, the Contractor shall maintain, preserve and make available to RTD and any of its authorized representatives access at all reasonable times to any books, documents, papers and records of Contractor which are directly pertinent to this Contract for the purposes of making audits, examinations, excerpts and transcriptions.

B. The Contractor shall maintain and RTD shall have the right to examine and audit all records and other evidence sufficient to reflect properly all prices, costs, or rates negotiated and invoiced in performance of this Contract. This right of examination shall include inspection at all reasonable times of the Contractor's offices engaged in performing the Contract.

C. If this Contract is completely or partially terminated, the Contractor shall make available, for a period of the longer of three years or such other time as required by another provision in this Contract after any resulting final termination settlement, the records relating to the Work completed up to the date of termination. The Contractor shall make available records relating to appeals under the Disputes clause or to litigation or the settlement of claims arising under or relating to this Contract until such appeals, litigation, or claims are finally resolved.

D. The Contractor shall insert this Article in all subcontracts under this Contract and require subcontractor compliance with this Article.

ARTICLE 11. PERFORMANCE OF WORK

A. Scope of Work. The Contractor shall provide RTD with the Work set forth in Section II, Scope of Work, as may be amended by change order or Contract amendment.

B. Notice to Proceed. The Contractor shall not commence performance of Work nor incur any costs for which Contractor intends to seek reimbursement until the date specified in the notice to proceed or, if no date is specified, until Contractor's receipt of notice to proceed.

C. Work Orders. If RTD specifies in writing that this Contract is a work-order contract, the Contractor shall not perform any Work except pursuant to a valid, fully executed work order, which shall be in a form prescribed by RTD. Each such work order shall be subject to the terms and conditions of this Contract. Any work order issued must contain a detailed summary of the Work to be performed, the projected cost for such Work, cost breakdown, completion date, an agreed-upon delivery schedule, and any other relevant information. To be valid, a work order must be signed by RTD and the Contractor; however, RTD and the Contractor shall not execute any work order if the cost authorized by the work order, when added to the cost of all previously executed work orders, will result in expenditures

in excess of the total consideration set forth on the Statement of Contract Cost, as may be amended by Contract amendment.

D. Costs Incurred by Contractor. The Contractor shall immediately notify RTD whenever it appears that costs necessary to perform the Work required will exceed the amount authorized by the Statement of Contract Cost. If the Work is performed pursuant to work order, the Contractor shall notify RTD whenever it appears that costs necessary to perform Work under any work order will exceed the amount authorized by the work order. The Contractor shall not incur any costs in excess of authorized amounts without written authorization from RTD. If RTD authorization is not forthcoming, the Contractor shall not be obligated to continue performance of the Work beyond the authorized amount. Nothing contained in this Contract shall allow the Contractor to exceed the total consideration set forth on the Statement of Contract Cost, as amended.

E. Time of Performance.

1. The Contractor shall complete the phases of Work in accordance with the agreed-upon Work schedule included in the Scope of Work or work orders, if any. The Work schedule shall include allowances for time required for RTD review and approval and for approvals of jurisdictional authorities. The Contractor shall not exceed the agreed-upon Work schedule, except for reasonable cause and immediate notice to RTD of delay or potential delay.
2. If the Contractor exceeds the Work schedule or fails to timely submit required Work as set forth on the Work schedule, RTD shall have the right to withhold payment, assess reasonable damages caused by the late submittal, and/or terminate this Contract in accordance its Termination provisions.
3. The Contractor shall immediately inform RTD of any delay in the Work that threatens to extend any deadline or timeframe set forth in the work orders or Work schedule.

F. Safety.

1. The Contractor shall be responsible for safety related to all aspects of the Work. The Contractor shall obtain all health, fire, and other relevant safety regulations, work practices, and procedures prescribed by law and by RTD and shall ensure that the Contractor's employees and subcontractors' employees are notified of, understand, and abide by them at all times. Unless otherwise agreed in this Contract, and at no cost to RTD, the Contractor shall provide all required personal protective equipment and other equipment required for the safe performance of the Work. If the Contractor fails to remedy any breach of this paragraph or fails to comply with any safety directive of RTD immediately after receipt of written notice, RTD may enter the Work site and effect such measures as may be necessary to secure compliance, in addition to any other remedies provided to RTD by this Contract. RTD shall have the right to deduct from any payment due to the Contractor an amount sufficient to reimburse RTD for securing such compliance.
2. The Contractor shall promptly report all accidents, safety incidents, injuries, and environmental incidents to RTD and to government authorities as required by law.

3. At any reasonable time, RTD may inspect a Work site and appropriate records regarding the Contractor's safety procedures and statistics to ascertain compliance with the safety requirements of this Contract. Neither the existence nor exercise of such right by RTD shall relieve the Contractor of its responsibility for compliance with, and for monitoring compliance by the Contractor and its subcontractors with, the safety requirements of this Contract.

4. The Contractor shall stop Work when an imminent hazard to persons, property, or the environment is identified and shall immediately notify RTD that Work has stopped, providing the reasons for stopping the Work and an estimate of when the Work will resume. The Contractor shall take all appropriate measures to abate the imminent hazard and limit the duration of the stoppage of Work. The Contractor shall coordinate efforts with RTD to mitigate the effect of the stoppage of Work.

5. The Contractor shall ensure all of its employees and subcontractors' employees understand their right to stop Work at any time they feel there is an unsafe condition or unsafe behavior in place that could harm them, others, property, or the environment. The Work shall not resume until all appropriate measures to abate the hazards have been implemented.

6. Notwithstanding any other provision of this Contract, RTD has the right to immediately suspend the performance of the Work if RTD, in its sole judgment, determines that any employee of the Contractor or subcontractors is failing to comply with RTD safety requirements or applicable safety laws and regulations while performing the Work, or if the safety of RTD employees or patrons is at risk or RTD operations are at risk. The suspension will continue until RTD notifies the Contractor that the suspension is lifted. The Contractor acknowledges that RTD has no obligation to lift the suspension until RTD is satisfied that the Contractor will comply with the Contract requirements. RTD shall not be liable for any delays in the completion of the Work that result from an RTD suspension under this paragraph.

ARTICLE 12. CHANGE ORDERS AND CONTRACT AMENDMENTS

A. **Change Orders**. RTD may at any time, by written order, and without notice to sureties, if any, make changes within the general scope of this Contract to the description of Work to be performed; the time allowed for performance; or the place of performance.

B. **Contract Amendments**. Any change, including a change described in the preceding paragraph, that causes an increase or decrease in the cost to perform the Work; increases the time allowed for performance of any part of the Work under this Contract by greater than 30 days; or otherwise materially affects any terms or conditions of this Contract shall not be effective unless made by written instrument signed by RTD's General Manager and the Contractor.

ARTICLE 13. QUALITY OF WORK

A. The Contractor shall perform the Work in accordance with all applicable federal, state and local laws, rules, regulations, and ordinances, as well as with the prevailing standard of practice normally exercised in the performance of work of a similar nature in Colorado, and shall bear all costs of such compliance. The Contractor shall be responsible for the professional quality, technical accuracy, and the coordination of all Work.

B. Neither RTD's review, approval, or acceptance of, nor payment for, the Work required under this Contract shall operate as a waiver of any rights under this Contract or of any cause of action arising out of the performance of this Contract, and the Contractor shall be and remain liable to RTD in accordance with applicable law for all damages to RTD caused by the Contractor's negligent performance of any of the Work furnished under this Contract.

C. If the Contractor is required to correct or re-perform defective or nonconforming Work, it shall be at no cost to RTD, and any Work corrected or re-performed by the Contractor shall be subject to this Article to the same extent as Work initially performed. If the Contractor fails or refuses to correct or re-perform Work, RTD may, by contract or otherwise, have an alternative contractor correct or re-perform the defective or nonconforming Work, and RTD shall charge to the Contractor the cost occasioned to RTD for the alternative contractor work or make an equitable adjustment in the Contract Cost. If defective or nonconforming Work is not required by RTD to be corrected or re-performed, RTD shall nevertheless make an equitable adjustment in the Contract Cost.

ARTICLE 14. WARRANTY

A. Contractor expressly warrants that all Work covered by this Contract shall conform to the Scope of Work upon which this Contract is based and shall conform to the prevailing standards of practice normally exercised in Colorado for the performance of work of a similar nature and under similar circumstances. Inspection, acceptance and use of the Work shall not affect the Contractor’s obligation under these warranties, and such warranties shall survive inspection, acceptance and use. Any inspection, acceptance or payment for Work by RTD shall not constitute a waiver by RTD of any warranties. These warranties shall run to RTD, its successors, and assigns.

B. Contractor represents and warrants that it has sufficiently informed itself in all matters affecting the performance of the Work, the furnishing of the Work, or any others material items specified in the Scope of Work. All personnel assigned by the Contractor to perform the Work shall be capable, skilled, qualified and competent to perform such Work. RTD may require Contractor to remove from the Work any employee, agent, or representative of Contractor that RTD deems incompetent, careless, or negligent.

C. Contractor further represents and warrants that the prices negotiated for this Contract are a complete and correct statement of Contractor’s prices for furnishing the Work and are not less favorable than those currently extended to any other customer for the same or like work in equal or smaller amounts.

D. The surety for the faithful performance bond, if any, required by this Contract is liable on its bond for all obligations of the Contractor, including warranty provisions.

ARTICLE 15. PROFESSIONAL REQUIREMENTS

A. Certification, Registration, and Licensing. The Contractor and all persons performing Work under this Contract on behalf of the Contractor shall be certified, registered or licensed as may be required by applicable state and federal laws governing the particular field of Work required or as may otherwise be required by the Contract.

B. Professional Associations. The Contractor may, with the prior written consent of RTD, join with it in the performance of this Contract any other duly licensed or registered contractors with whom it may in good faith enter into an association. In the event there is a dissolution of a professional association, other than by death of a member, RTD shall designate which former member shall continue with the Work and may make all payments thereafter due in connection with the Work directly to the person or persons so designated and without being required to look to the application of payments as among former members. In the event of the death of one member of an association, the surviving member or members of the association, as an association, shall succeed to the rights and obligations of the original association under the Contract.

C. Subcontractors and Consultants. If consulting services are to be performed by professionals in the Contractor's employ, then such services must currently be and have been regularly a service of the Contractor's organization. In the event the Contractor does not have certain professional consultants and consulting services as part of its regular staff and services, such consulting services shall be performed by practicing professional consultants. All professional consultants, staff or practicing, must be retained for the life of the project, provided however that acceptable replacements must be approved in writing by RTD. Prior to designating a professional to perform any consulting services, the Contractor shall submit the name of such professional, together with a résumé of his or her training and experience in work of like character and magnitude of the project being contemplated, to RTD and receive approval in writing from RTD.

ARTICLE 16. KEY PERSONNEL AND CONTRACTOR REPRESENTATIVES

A. Key Personnel. The personnel listed on Exhibit 1 are considered to be essential to the Work. Prior to removing any key personnel from Contract Work, the Contractor shall notify RTD within 14 days of such proposed removal and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the Contract. The Contractor shall not remove key personnel without the written consent of RTD by Contract amendment.

B. The Contractor Representative(s). The Contractor may designate one or more representatives to administer this Contract and to have overall direction and control over the Work to be performed by the Contractor. Any representative(s) so designated under this provision shall personally supervise and control the Work to be performed by the Contractor. The Contractor shall notify RTD of the names and contact information of any designated Contractor representatives.

ARTICLE 17. WORK OVERSIGHT BY RTD

A. RTD shall have the right to review at all reasonable times any Work. The extent and character of the Work shall be subject to the general oversight, supervision, direction, control, and approval of RTD.

B. Upon substantial completion of the Work, the Contractor shall submit the Work for RTD's review and RTD shall notify the Contractor of its acceptance or rejection. If approved, RTD shall provide to the Contractor written approval for any or all portions of the Work. RTD shall have the right to reject any Work that is not consistent and compatible with the Scope of Work. If RTD rejects any Work, RTD shall promptly notify the Contractor in writing of the grounds for rejection and offer suggestions for correcting the problem. RTD shall re-review and comment on the revised Work within a reasonable period of time.

C. Any approval, review, inspection, direction or instruction by RTD, or any party on behalf of RTD, in respect to the Work relates only to the results RTD desires to obtain and shall in no way affect the Contractor's independent contractor status or obligation to perform in accordance with this Contract.

ARTICLE 18. OWNERSHIP OF MATERIALS AND DOCUMENTS

A. RTD-Furnished Materials. RTD shall make available to the Contractor, to the extent permitted by law, all materials and information collected, compiled, or developed by RTD staff, consultants, planning organization, or municipalities necessary to perform under this Contract. All such material furnished to the Contractor shall be used by it only in connection with the performance of this Contract, and title to such material shall at all times remain in RTD. Upon termination or completion of this Contract, all such material shall be returned promptly to RTD.

B. Subject Data Created or Supplied by the Contractor or Consultants.

1. The term "Subject Data" used in this Article means recorded information, whether or not copyrighted, that is delivered or specified to be delivered under the Contract. "Subject Data" includes graphic or pictorial delineation in media such as drawings or photographs; text in specifications or related performance or design-type documents; machine forms such as punched cards, magnetic tape, or computer memory printouts; and information retained in computer memory. Examples include but are not limited to computer software, engineering drawings and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog item identifications, and related information. "Subject Data" does not include financial reports, cost analyses, and similar information incidental to Contract administration.

2. All Work required under this Contract, including Work in electronic form, prepared by the Contractor and the Contractor's consultants is Subject Data for use solely with respect to the Work. To the extent permitted by law, RTD shall be deemed the owner of all Subject Data created under this Contract. Furthermore, the Contractor assigns to RTD the entire right, title, and interest in and to copyrights in all Subject Data and all works based upon, derived from, or incorporating the Subject Data; all copyright applications, registrations, extensions, or renewals relating to all Subject

Data and all works based upon, derived from, or incorporating the Subject Data; and all moral rights or similar rights with respect to the Subject Data throughout the world.

3. The Contractor retains the exclusive rights, title, and ownership to any and all pre-existing materials owned or licensed to the Contractor including, but not limited to, all pre-existing software, licensed products, associated source code, machine code, text images, audio and/or video, and third-party materials, delivered by the Contractor under the Contract, whether incorporated in the Work or necessary to use the Work (collectively, "Contractor Property"). The Contractor Property shall be licensed to RTD as set forth in this Contract or an RTD-approved license agreement (i) entered into as an exhibit or attachment to this Contract; (ii) obtained by RTD from the applicable third-party vendor; or (iii) in the case of open source software, the license terms set forth in the applicable open source license agreement.

4. If a court of competent jurisdiction finds the Contractor to be the owner of any Subject Data created under this Contract, RTD shall automatically be granted a perpetual nonexclusive, royalty-free, and irrevocable license to reproduce and use, and permit others to reproduce and use solely for RTD's internal use, all Subject Data created under this Contract solely for the purposes of performing the Work or for future alterations or additions to the Work. The Contractor shall obtain similar nonexclusive licenses from the Contractor's consultants consistent with this Contract. RTD may assign and license its rights under this license. If and upon the date the Contractor is adjudged in default of this Contract, the foregoing license shall be deemed terminated and replaced by a second, nonexclusive license permitting RTD to authorize other similarly credentialed professionals to reproduce and, where permitted by law, to make changes, corrections or additions to the Subject Data solely for purposes of completing, using and maintaining the Work or for future alterations or additions to the Work.

5. In addition, the Contractor grants to RTD (and to recipients of the Work distributed by or on behalf of RTD) a perpetual, worldwide, no-charge, royalty-free, irrevocable patent license to make, have made, use, distribute, sell, offer for sale, import, transfer, and otherwise utilize, operate, modify and propagate the contents of the Work. Such license applies only to those patent claims licensable by the Contractor that are necessarily infringed by the Work alone, or by the combination of the Work with anything else used by RTD.

6. Whether or not the Contractor is under contract with RTD at the time, the Contractor shall execute applications, assignments, and other documents, and shall render all other reasonable assistance requested by RTD, to enable RTD to secure patents, copyrights, licenses and other intellectual property rights related to the Work. The Parties intend the Work to be works made for hire. The Contractor assigns to RTD and its successors and assigns the entire right, title, and interest in and to all causes of action, either in law or in equity, for past, present, or future infringement of intellectual property rights related to the Work and all works based on, derived from, or incorporating the Work.

7. Any unilateral use by RTD of the Subject Data for completing, using, maintaining, adding to or altering the Work shall be at RTD's sole risk and without liability to the Contractor and the Contractor's consultants, provided however that if RTD's unilateral use occurs for completing, using or maintaining the Work as a result of the Contractor's breach of this Contract, nothing in this Article shall be deemed to relieve the Contractor of liability for its own acts or omissions or breach of this Contract.

C. Indemnification. The Contractor shall indemnify and save and hold harmless RTD, its officers, agents, and employees acting within the scope of their official duties against any liability, including costs and expenses, resulting from any violation by the Contractor of proprietary rights, copyrights, or rights of privacy arising out of the publication, translation, reproduction, delivery, performance, use, or disposition of any materials furnished by either party under this Contract.

ARTICLE 19. INSURANCE AND BOND REQUIREMENTS

The Contractor shall maintain in full force and effect insurance in the amounts and coverages defined on Exhibit 2. The Contractor shall maintain any bonds required by applicable state or federal law regulating the particular field or profession. Bonds specifically required by RTD under this Contract are set forth on Exhibit 2.

ARTICLE 20. HOLD HARMLESS

A. The Contractor shall defend, indemnify, and hold harmless RTD, its directors, managers, employees, agents and assigns from and against any and all claims, suits, demands, damages, liabilities, settlements, and court awards including costs, expenses, and reasonable attorneys' fees, to the extent such claims are caused, in whole or in part, by any act or omission of, or breach of contract by, the Contractor, its employees, agents, subcontractors or assignees arising from, related to, in connection with, or in any way involving the performance of this Contract, but not to the extent such claims are caused solely by any act or omission of, or breach of contract by RTD, its directors, managers, employees, agents, or other contractors or assignees, or other parties not under the control of or responsible to the Contractor.

B. The Contractor shall give RTD immediate written notice of any suit or action filed or of any claim made against the Contractor, its employees, agents, subcontractors or assignees arising from, related to, in connection with or in any way involving the performance of this Contract. The Contractor shall immediately furnish to RTD copies of all pertinent papers received by the Contractor. If the amount of the liability claimed exceeds the amount of the Contractor's insurance coverage against such claim, the Contractor shall authorize and direct the Contractor's counsel and the Contractor's insurer(s), if any, to collaborate and cooperate with RTD representatives in settling or defending such claim.

C. The duties, obligations, rights, and remedies provided by the Contract shall be in addition to and not a limitation of any duties, obligations, rights and remedies otherwise imposed or available by law.

D. If the Contractor is comprised of more than one legal entity, each such entity shall be jointly and severally liable under the Contract.

E. Notwithstanding any other provision of this Contract to the contrary, no term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions of the Colorado Governmental Immunity Act, C.R.S. § 24-10-101, et seq., as amended.

ARTICLE 21. TERMINATION

A. For Convenience. RTD may, by giving at least 14 days' written notice to the Contractor, terminate this Contract, or suspend performance under this Contract, in whole or in part and at any time for RTD's convenience. The Contractor shall be compensated solely for Work satisfactorily performed prior to the effective date and time of termination or suspension. The Contractor shall have no right to recover lost profits on the balance of the Work or any other measure of damages.

B. For Default. RTD may declare default in the Contractor's performance of any term of this Contract by giving seven days' written notice to the Contractor specifying with particularity the basis for such default. The Contractor shall deliver a response in writing to RTD within five days of Contractor's receipt of RTD's default notice, setting forth a reasonable proposal to cure or to prevent repetition of the default. If the Contractor fails to timely respond to the notice of default, fails to cure the default, or if the default occurs again on any Work performed (or which should have been performed) during the remainder of the Contract term (including options), RTD shall have the right to terminate this Contract in whole or in part for default by written notice. RTD is not required to provide subsequent written notices of default for recurring instances of default already brought to the attention of the Contractor in a written notice. In the event of termination for default, the Contractor shall be compensated solely for Work satisfactorily performed prior to the effective date and time of termination. RTD may proceed with the Work by contract or otherwise, and the cost to RTD of completing the Work shall be charged to the Contractor or deducted from any sum due the Contractor. If after termination for default it is determined that the Contractor was not in default, the rights and obligations of the parties shall be the same as if the termination had been issued for RTD's convenience.

C. Suspension of Work. RTD may suspend the Contractor's performance of the Work by giving the Contractor seven days' written notice. Upon Contractor's receipt of notice of suspension of Work, the Contractor shall perform no further Work, and RTD will not be required to reimburse the Contractor for any costs incurred subsequent to Contractor's receipt of notice of suspension and prior to RTD's notice to resume Work, if any. Suspension of Work may be in whole or in part, as specified by RTD. The Contractor shall continue to submit invoices for Work performed prior to Contractor's receipt of notice of suspension of Work. If after six months of suspension RTD has not given the Contractor notice to resume Work, the Contractor is entitled to request in writing that RTD either (1) amend the Statement of Contract Cost or (2) terminate the Contract pursuant to the "For Convenience" provision of this Article. If suspension for more than six months is not due in any part to the fault of the Contractor, RTD shall be required to amend or terminate the Contract. No amendment to the Statement of Contract Cost shall be made under this

Article if suspension, delay, or interruption of the Work is due to the fault or negligence of the Contractor, or for which an equitable adjustment is provided for or excluded under any other term or condition of this Contract.

ARTICLE 22. EXCUSABLE DELAY

A. The Contractor shall not be in default by reason of any failure in performance of this Contract in accordance with its terms (including any failure by the Contractor to make progress in the execution of the Work, which endangers such performance) if such failure arises out of unforeseeable causes beyond the control and without the fault or negligence of the Contractor, provided that the Contractor shall within five days of the start of any such failure, potential delay, or default notify RTD in writing of the causes of the failure, potential delay, or default and the related facts. Such causes may include, but are not restricted to, acts of God or of public enemy, acts of government in its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather.

B. If failure to perform is caused by the failure of a subcontractor to perform or make progress, and if such failure arises out of unforeseen causes beyond the control of both the Contractor and subcontractor, and without the fault or negligence of either of them, the Contractor shall not be deemed to be in default, unless:

1. The Work to be furnished by the subcontractor was obtainable from other sources at a price acceptable to RTD;
2. RTD has ordered the Contractor in writing to procure such Work from such other sources; and
3. The Contractor fails to comply with such order.

C. Upon request of the Contractor, RTD shall ascertain the facts and extent of a failure to perform. If RTD determines that any failure to perform is excusable under this Article, RTD may revise the schedule of Work, subject to RTD's rights under the Article entitled "Termination."

ARTICLE 23. DISPUTES

A. Except as otherwise provided in this Contract, any dispute arising under this Contract concerning a question of fact that is not disposed of by agreement shall be decided by RTD's General Manager or his or her delegate. Contractor will be notified of the decision in writing. To the extent allowable by law, any such decision shall be final, conclusive, and not subject to judicial review unless shown to be fraudulent, capricious, arbitrary, or so grossly erroneous as to imply bad faith.

B. This Article does not preclude judicial consideration of questions of law. Nothing in this Contract shall be construed as making final the decision of any administrative official, representative, or board on a question of law.

C. All costs, expenses and attorney fees of the Contractor of any appeal, suit or claim brought by the Contractor shall be paid by the Contractor.

D. Unless otherwise directed by RTD, the Contractor shall continue performance under this Contract while matters in dispute are being resolved.

ARTICLE 24. PROHIBITED INTERESTS

A. **The Contractor's Interest**

1. The Contractor shall not knowingly perform any act that would conflict in any manner or degree with the performance of Work under this Contract. The Contractor shall not knowingly employ any person when such employment would cause such a conflict.
2. Wherever the Contractor prepares or assists RTD in the preparation of a statement of work, work program, or system specifications to be used in a competitive procurement by RTD, the Contractor will be ineligible to supply the same in connection with such procurement. The Contractor may otherwise compete for RTD business on an equal basis with other parties.
3. These restrictions shall apply until the closing of the Contract and with respect to any future change orders or Contract amendments.

B. **Officials and Employees Not To Benefit**

1. No member of or delegate to Congress, or resident commissioner, shall be admitted to any share or part of this Contract or to any benefit arising from it.
2. No employee of RTD or any member of its governing body shall have any personal or financial interest, direct or indirect, in this Contract or any contract executed subsequently in connection with this Contract during his or her tenure or for one year thereafter. No director, officer, employee, or agent of RTD shall be interested in any contract or transaction with RTD except in his or her official representative capacity.

C. **Gratuities**

1. This Contract and any other RTD contract with the Contractor may be terminated by written notice if RTD determines that the Contractor, its agent, or another representative:
   a. Offered or gave a gratuity to a director or employee of RTD; and,
   b. Intended, by the gratuity, to obtain a contract or favorable treatment under a contract.

D. **Termination; Remedies.** If this Contract is terminated due to breach of this Article, RTD is entitled to pursue the same remedies as in a termination for default. RTD shall not, however, be required to provide the Contractor with opportunity to cure the default.

ARTICLE 25. BANKRUPTCY

If the Contractor enters into proceedings relating to bankruptcy, whether voluntary or involuntary, the Contractor agrees to furnish to RTD, by certified mail, notification of the bankruptcy within five days of the initiation of the proceedings relating to bankruptcy

filing. Such notice shall include (i) the date on which the bankruptcy petition was filed, (ii) the identity of the court in which the bankruptcy petition was filed, and (iii) a listing of contract numbers for all RTD contracts against which final payment has not been made. This obligation remains in effect until the closing of the Contract.

ARTICLE 26. NOTICES

Unless otherwise specified in this Contract, notices required to be given by RTD or the Contractor under this Contract must be provided in writing and delivered by e-mail, facsimile, hand delivery or by U.S. Mail, first class, postage pre-paid, to the party representatives identified on the Contract Award and Signature Page. Notices sent by first class mail shall be deemed to have been received five days after having first been placed in the mail. Notice shall not be deemed given if not provided in the manner prescribed in this Article.

ARTICLE 27. APPROPRIATIONS

All obligations of RTD under this Contract that require funding are subject to prior annual appropriations of monies expressly made by the Board of Directors of RTD for the purposes of this Contract. Nothing in this Contract shall be construed by either the Contractor or RTD as a multiple fiscal year obligation as described by Article X, Section 20 of the Colorado Constitution. If funding is not appropriated by the Board of Directors, RTD may terminate or modify the Contract as required. Additional funding to the Contract will be accomplished by a Contract amendment. No legal liability on the part of RTD for any payment may arise for performance under this Contract beyond the current funding year, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability.

ARTICLE 28. SMALL-BUSINESS ENTERPRISES

The Contractor shall cooperate with RTD with regard to maximum utilization of minority-owned businesses and/or small-business enterprises ("SBEs") and will use its best efforts to ensure that minority-owned businesses and SBEs have the maximum practicable opportunity to compete for subcontract Work under this Contract. When no SBE participation goal is set under the Contract, but the Contractor utilizes SBE subcontractor(s), the Contractor may, but is not required to, submit the following information to RTD's Small Business Office: the names of RTD-certified SBE subcontractor(s) that have performed Work under the Contract; a description of the Work performed by the SBE subcontractor(s); and an itemization or summary of the payments made to the SBE subcontractor(s) for Work under the Contract.

ARTICLE 29. CONFIDENTIALITY

A. In this Article, "Information" means all information relating to RTD that is supplied by or on behalf of RTD (whether before or after the Effective Date of this Contract), either in writing, orally or in any other form, directly or indirectly, from or pursuant to discussions

with the Contractor or which is obtained through observations made by the Contractor, including all work products, deliverables, analyses, compilations, studies and other documents, whether prepared by or on behalf of RTD, which contain or otherwise reflect or are derived from such information.

B. The Contractor shall maintain the confidentiality of any Information, except that Information may be disclosed or provided by the Contractor:

1. to directors, officers, employees, consultants and agents of the Contractor, including accountants, legal counsel and other advisors;
2. to any subcontractors to the extent such Information is necessary for the performance by the subcontractor of its obligations under this Contract; or
3. to the extent:
    a. it is required to disclose such Information pursuant to federal, state or local law or by any subpoena or similar legal process or by any federal, state or local authority exercising jurisdiction over the Contractor;
    b. RTD confirms in writing that such Information is not required to be treated as confidential; or
    c. such Information is or comes into the public domain otherwise than through any disclosure prohibited by this Contract; and

provided that, in the cases of paragraphs B.1., B.2, and B.3, the persons to whom such disclosure is made will be informed of the confidential nature of such Information and will so receive such Information subject to the same or similar requirements to maintain confidentiality as contained in this Contract.

C. The Contractor understands that any documents that it creates, supplies to RTD or for which the Contractor acts as custodian for RTD under this Contract are subject to public inspection and copying under the Colorado Open Records Act, C.R.S. § 24-72-201, et seq., unless exempt from public disclosure by law. The Contractor agrees that if it considers any such documents to be exempt from public disclosure, it will mark each such document as exempt, identifying the specific provision of law under which the Contractor is claiming exemption of such document from public disclosure. The Contractor further agrees that if a Colorado Open Records Act request is filed with RTD seeking disclosure of any documents created by the Contractor, supplied to RTD, or held by the Contractor for RTD under this Contract, the Contractor will, if necessary, assist RTD in responding to the request by locating any documents requested and providing them to RTD within 24 hours, unless otherwise agreed in writing by RTD. The Contractor agrees to hold RTD harmless and, at RTD's option, indemnify and provide legal defense for RTD from all claims and demands, including paying all attorneys' fees, asserted against RTD that result from (i) the Contractor's failure to supply documents to RTD or (ii) from RTD's refusal to make public any documents the Contractor has designated as exempt. The Contractor also agrees that, if any action is filed in court seeking disclosure of exempt documents, RTD may deposit the documents with the court and the Contractor will defend in court its designation of the information as exempt from disclosure.

D. The Contractor shall not use RTD technology, data or Information to perform an illegal act, nor share any password or account access provided exclusively to the Contractor. The

Contractor shall not attempt to use or obtain access codes in an unauthorized manner or from another user. The Contractor shall not allow non-employees to access RTD computer systems, unless otherwise specifically allowed by RTD.

E. The Contractor acknowledges that the faithful compliance with this Article is necessary to protect RTD and that any action inconsistent with this Article or with any RTD policy and procedure will cause RTD irreparable and continuing harm. Therefore, the Contractor consents to RTD obtaining a court order to enjoin any action inconsistent with the provisions of this Article without RTD having to post any bond or security for such order.

ARTICLE 30. ACCESS REQUIREMENTS FOR PERSONS WITH DISABILITIES

A. RTD must comply with: 49 U.S.C. § 5301(d), which states the federal policy that elderly individuals and individuals with disabilities have the same right as other individuals to use public transportation services and facilities, and that special efforts shall be made in planning and designing those services and facilities to implement transportation accessibility rights for elderly individuals and individuals with disabilities; all applicable provisions of section 504 of the Rehabilitation Act of 1973, as amended; 29 U.S.C. § 794, which prohibits discrimination on the basis of disability; the Americans with Disabilities Act of 1990 (ADA), as amended; 42 U.S.C. §§ 12101, et seq., which requires that accessible facilities and services be made available to individuals with disabilities; and the Architectural Barriers Act of 1968, as amended, 42 U.S.C. §§ 4151, et seq., which requires that buildings and public accommodations be accessible to individuals with disabilities.

B. All Work provided by the Contractor for RTD under this Contract shall comply with the above-referenced laws as well as all other applicable federal, state and local regulations and directives and any subsequent amendments.

ARTICLE 31. ENERGY CONSERVATION

Contractor agrees to comply with mandatory standards and policies relating to energy efficiency that are contained in the state energy conservation plan, if any, issued in compliance with the Energy Policy and Conservation Act.

ARTICLE 32. CLEAN WATER

A. Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. § 1251, et seq. Contractor agrees to report each violation to RTD and understands and agrees that RTD will, in turn, report each violation as required to assure notification to the appropriate EPA Regional Office or the appropriate Colorado Department of Public Health and Environment department.

B. Contractor also agrees to include these requirements in each subcontract entered into for performance of Work under this Contract.

ARTICLE 33. CLEAN AIR

A. Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. §§ 7401, et seq. Contractor agrees to report each violation to RTD and understands and agrees that RTD will, in turn, report each violation as required to assure notification to the appropriate EPA Regional Office or the appropriate Colorado Department of Public Health and Environment department.

B. Contractor also agrees to include these requirements in each subcontract entered into for performance of Work under this Contract.

ARTICLE 34. CIVIL RIGHTS

A. Nondiscrimination. In accordance with Title VI of the Civil Rights Act, as amended, 42 U.S.C. § 2000d, Section 303 of the Age Discrimination Act of 1975, as amended, 42 U.S.C. § 6102, Section 202 of the Americans with Disabilities Act of 1990, 42 U.S.C. § 12132, and federal transit law at 49 U.S.C. § 5332, Contractor agrees that it will not discriminate against any employee or applicant for employment because of race, color, creed, national origin, sex, age, or disability. In addition, Contractor agrees to comply with applicable federal implementing regulations.

B. Equal Employment Opportunity.

1. Race, Color, Creed, National Origin, Sex. In accordance with Title VII of the Civil Rights Act, as amended, 42 U.S.C. § 2000e, and federal transit laws at 49 U.S.C. § 5332, Contractor agrees to comply with all applicable equal employment opportunity requirements of U.S. Department of Labor regulations, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor," 41 CFR Parts 60, et seq., (which implement Executive Order No. 11246, "Equal Employment Opportunity," as amended by Executive Order No. 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," 42 U.S.C. § 2000e note), and with any applicable federal statutes, executive orders, regulations, and federal policies that may in the future affect construction activities undertaken in the course of the Contract. Contractor agrees to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, creed, national origin, sex, or age. Such action shall include, but not be limited to, the following: employment, upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship. In addition, Contractor agrees to comply with any federal implementing requirements.
2. Age. In accordance with Section 4 of the Age Discrimination in Employment Act of 1967, as amended, 29 U.S.C. § 623 and federal transit law at 49 U.S.C. § 5332, Contractor agrees to refrain from discrimination against present and prospective employees for reason of age. In addition, Contractor agrees to comply with any federal implementing requirements.
3. Disabilities. In accordance with Section 102 of the Americans with Disabilities Act, as amended, 42 U.S.C. § 12112, Contractor agrees that it will comply with the

requirements of U.S. Equal Employment Opportunity Commission, "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 CFR Part 1630, pertaining to employment of persons with disabilities. In addition, Contractor agrees to comply with any federal implementing requirements.

C. Contractor also agrees to include these requirements in each subcontract entered into for performance of Work under this Contract.

ARTICLE 35. INDEPENDENT CONTRACTOR

A. The Contractor shall perform its duties under this Contract as an independent contractor and not as an employee of RTD. **Unless otherwise expressly provided in this Contract, neither the Contractor nor any agent or employee of the Contractor shall be an agent or representative of RTD. Neither the Contractor nor any agent or employee of the Contractor shall be an employee or servant of RTD. Nothing contained in the Contract Documents or otherwise creates any partnership, joint venture, or other association or relationship between RTD and the Contractor.** Any approval, review, inspection, direction or instruction by RTD or any party on behalf of RTD in respect to the Work of the Contractor shall relate to the results RTD desires to obtain from the Work, and shall in no way affect the Contractor's independent contractor status or obligation to perform the Work in accordance with the Contract Documents. The Contractor has no authorization, express or implied, to bind RTD to any agreements, liability, or understanding except as expressly set forth in this Contract.

B. **The Contractor shall pay when due all federal and state taxes and contributions for Social Security, unemployment insurance, income withholding tax, and other taxes measured by wages paid to the Contractor's employees, as well as all sales, consumer, employment, use and similar taxes for the Work or portions of the Work provided by or through the Contractor or any subcontractor or vendor or relating to their operations or property. The Contractor acknowledges that the Contractor and its employees are not entitled to workers' compensation benefits or unemployment insurance benefits unless the Contractor or third party provides such coverage, and that RTD does not pay for or otherwise provide such coverage. The Contractor shall provide and keep in force workers' compensation (and provide proof of such insurance when requested by RTD) and unemployment compensation insurance in the amounts required by law, and shall be solely responsible for the acts of the Contractor, its employees and agents.**

ARTICLE 36. SUCCESSORS AND ASSIGNS

The Contractor shall not assign rights or delegate duties under this Contract (or subcontract any part of the performance required) without the express, written consent of RTD. This provision shall not prohibit assignments of the right to payment to the extent permitted by law, provided that RTD receives written notice of assignment adequate to

identify the rights assigned. Such assignment shall not be valid until RTD receives the required notice, and the Contractor assumes this risk.

ARTICLE 37. REASONABLENESS OF CONSENT OR APPROVAL

Whenever the approval or consent of RTD is called for under this Contract, RTD shall be entitled to consider public and governmental policy in reasonably granting or denying such approval. Subject to the foregoing, required approvals or consent shall not be unreasonably withheld.

ARTICLE 38. NO THIRD PARTY BENEFICIARIES

This Contract shall inure to the benefit of and be binding only upon the parties and their successors and assigns. The enforcement of the terms and conditions of this Contract and all rights of action relating to such enforcement shall be strictly reserved to the parties to the Contract. No other person or entity shall have any claim or right of action as a Contract beneficiary; all such non-parties shall be incidental beneficiaries only.

ARTICLE 39. EXTENT OF AGREEMENT

This Contract represents the entire agreement between RTD and the Contractor and supersedes all prior negotiations, representations or agreements, either written or oral. This Contract may be amended only by written instrument signed by RTD's General Manager and the Contractor.

ARTICLE 40. COUNTERPARTS

This Contract may be executed in two or more counterparts, each of which shall be deemed an original having identical legal effect, and all of which together constitute the same instrument.

ARTICLE 41. INTERPRETATION OF CONTRACT

In the event of any ambiguity, n the Contractor's interpretation of any provision of this Contract shall not be binding on RTD unless that interpretation is one which has been furnished in writing by RTD. No alteration of or insertion into this Contract shall be binding on RTD unless expressly referenced in Exhibit 3. No RTD employee or agent has the authority to waive, modify or alter any provision in this Contract.

ARTICLE 42. SEVERABILITY

If any part of this Contract is held by any court of competent jurisdiction to be illegal or in conflict with any federal law or law of the State of Colorado, the validity of the remaining parts shall not be affected, and the rights and obligations of the Contractor and RTD shall be construed and enforced as if the Contract did not contain the invalid part.

ARTICLE 43. AUTHORITY

Each person executing this Contract expressly represents and warrants that he or she has been duly authorized by one of the parties to execute the Contract and to bind the party to the Contract terms and conditions.

ARTICLE 44. GOVERNING LAWS; JURISDICTION AND VENUE

The laws, regulations and rules of the State of Colorado govern the interpretation, execution and enforcement of this Contract without application of any choice of law rules that would apply the laws of any other state. Exclusive venue for any action related to performance of this Contract shall be the District Court of the City and County of Denver, State of Colorado.

ARTICLE 45. WAIVER

The waiver of any breach of a Contract term shall not be a waiver of any other term, or of the same term upon subsequent breach.

ARTICLE 46. ELECTRONIC SIGNATURES

This Contract may be executed by electronic signature, which shall be considered as an original signature for all purposes and shall have the same force and effect as an original signature. Without limitation, “electronic signature” shall include faxed versions of an original signature, electronically scanned and transmitted versions of an original signature, and digital signatures.

TECHNOLOGY TERMS AND CONDITIONS

DEFINITIONS

“Final Acceptance” means (i) if applicable, the Product has passed User Acceptance Testing and System Acceptance Testing as such terms and processes are described in the Scope of Work; (ii) all documentation has been provided to RTD; and (iii) RTD has provided written notice of acceptance of the Product.

"Intellectual Property Rights" means copyright, rights related to or affording protection similar to copyright, patents and rights in inventions, trade and service marks, logos, rights in internet domain names and website addresses and other rights in trade or business names, design rights (whether registerable or otherwise) and registered designs, know-how, trade secrets and moral rights and other similar proprietary rights or obligations, together with applications for registration and the right to apply for registration, and all other proprietary rights whether registerable or not having equivalent or similar effect in any country or jurisdiction and the right to sue for passing off in each case which may subsist or come into existence from time to time.

“Personally Identifiable Information (PII)” means any information that alone or in conjunction with other information could be used to identify or locate an individual.

“Product” means the goods or supplies and any related services provided to RTD by the Contractor under this Contract, including but not limited to software, hardware, technology applications or systems, and associated documentation.

“RTD Data” means all information processed or stored on computers or other electronic media by RTD or on RTD’s behalf, or provided to Contractor for such processing or storage, as well as information derived from such information. RTD Data includes, without limitation: (i) information on paper or other non-electronic media provided to Contractor for computer processing or storage, or information formerly on electronic media; (ii) information provided to Contractor by RTD customers, users, employees, or other third parties; and (iii) Sensitive RTD Data.

“Sensitive RTD Data” means data that poses a risk to RTD, its employees, customers, and the public if improperly disclosed or accessed, including without limitation personally identifiable information, financial information, protected health information, proprietary information, critical infrastructure information, security sensitive information, and other confidential information.

ANNUAL REPORTING REQUIREMENTS

A. SOC 2 Type 2 Report. Fourteen calendar days after receipt of the notice to proceed, Contractor shall provide to RTD its most recent Service Organization Control (SOC) 2 Type 2 report pertaining to the Scope of Work. Thereafter for the term of this Contract, the Contractor shall provide an updated SOC 2 Type 2 report to RTD on an annual basis. Practices used to maintain security in accordance with these terms and conditions must be included in the report. If Contractor fails to provide an updated report, then Contractor will notify RTD in writing of a date when the report will be made available to RTD, except that the updated report must be made available to RTD no later than 18 months after the last report was provided to RTD. If Contractor's SOC 2 Type 2 report is qualified, then Contractor will notify RTD in writing of the actions it is taking to correct any findings and the expected resolution date for those corrections. Should a SOC 2 Type 2 report not be performed or available, an alternative third-party control audit report may be acceptable to RTD with prior notice, sufficiency of criteria review, and approval from RTD. Contractor will be responsible for any and all costs associated with complying with this provision.

B. PCI-DSS Compliance. During the term of this Contract, the Contractor shall submit to RTD annually a PCI-DSS Service Provider Report on Compliance or Attestation of Compliance. Contractor shall deliver the results of the PCI compliance assessment in a format appropriate to the in-scope transaction quantity and scope of services under the PCI Standards. Contractor will be responsible for any and all costs associated with complying with this provision.

REGULATORY COMPLIANCE

A. Compliance at Delivery. The Contractor represents and warrants that the Product(s) delivered under this Contract complies with all applicable federal, state and local laws, rules, regulations, and ordinances, as well as with prevailing industry standards, including but not limited to:

   i. Payment Card Industry Data Security Standards (PCI-DSS)
   ii. Health Insurance Portability and Accountability Act (HIPAA)
   iii. Americans with Disabilities Act (ADA)

B. Future Compliance. For the term of this Contract, including any applicable maintenance and support periods, the Contractor shall ensure that the Product(s) remains in compliance with all applicable federal, state and local laws, rules, regulations, and ordinances, as well as with prevailing industry standards, including but not limited to:

   i. Payment Card Industry Data Security Standards (PCI-DSS)
   ii. Health Insurance Portability and Accountability Act (HIPAA)
   iii. Americans with Disabilities Act (ADA)

   Contractor's failure to ensure the Product(s) remains in compliance with the above-referenced standards will constitute a material breach of the Contract.

C. Costs. Contractor will pay for any and all costs associated with an audit or to gain compliance with these standards.

LIQUIDATED DAMAGES

A. Due to the nature and significance of the Work, the Contractor and RTD agree that a failure to perform the Work likely will result in severe loss to RTD. In addition, the Contractor and RTD also agree that it is extremely difficult to fix actual damages that may result from such failure to perform the Work. Consequently, this Contract allows for certain Liquidated Damages, as set forth in this Article, for certain failures to perform the Work.

Service Level Agreements.

1. RTD may assess Contractor for Liquidated Damages monthly at a rate of $3000.00] for each month that the Contractor fails to meet the Service Level Agreement ("SLA") threshold of 12 months for final delivery of the product and product deliverables. The estimated timeline for each phase is identified below.
    i. Phase I: Design, Architecture, Content – 3 months
    ii. Phase II: Development – 6-8 months
    iii. Phase III: Final Delivery – 1 month

Unresolved Tickets.

1. RTD may assess Contractor for Liquidated Damages monthly at a rate of $200.00 for each day during that month that 10 or more service tickets remain unresolved for a period of 30 days or more.
2. RTD may assess Contractor for Liquidated Damages monthly at a rate of $200.00 for each day during that month that a service ticket remains unresolved for a period of 180 days or more.]

B. The Contractor's liability as to any single failure to perform that portion of the Work identified in this Article for which a Liquidated Damage is affixed is limited to and fixed at the sum of Liquidated Damages provided in this Contract. Assessment of Liquidated Damages does not constitute a waiver of RTD's right to terminate the Contract for default for ongoing or systematic failures to perform the Work (see Article titled "Termination") or any other failure to perform the Work for which RTD has not assessed Liquidated Damages or not specifically identified in this Contract.

C. The RTD Contract Administrator or designee may assess Liquidated Damages as they are identified. RTD will give written notice of such assessment to the Contractor. The Contractor must respond to the RTD Contract Administrator or designee in writing within 14 calendar days for the response to be considered. Contractor's response must provide a reason why Liquidated Damages should not be assessed and, if available, provide supporting documentation. The RTD Contract Administrator or designee will make a final determination on the Liquidated Damages assessed based upon any information reasonably available to RTD. The Contractor is prohibited from appealing the assessment of Liquidated Damages or seeking dispute resolution regarding the assessment of Liquidated Damages pursuant to any other provision of this Contract.

D. RTD reserves the right, at its sole discretion, to excuse the imposition of Liquidated Damages; an excuse will not constitute a waiver of any subsequent assessment of Liquidated Damages. The assessment of Liquidated Damages will not relieve the Contractor of its obligations to

provide the Work and will not constitute a waiver or limitation of any other rights or remedies of RTD.

E. At RTD's sole option, Liquidated Damages may be subtracted from any payment currently due to the Contractor or that may become due to the Contractor in the future.

DATA MANAGEMENT

In the event of any conflict between this Article and other terms and conditions of the Contract, this Article shall control.

A. Confidential and Sensitive Data. If applicable and necessary under the Scope of Work, RTD shall define and/or approve (if generated or defined by the Contractor) what confidential and sensitive RTD Data may be created, collected, processed, transferred, or stored by the systems or processes supported by the Contractor such that it can be protected per these terms and conditions. Only the least amount of RTD Data required to perform the Work may be created or collected.

B. Privacy. Upon RTD's request, the Contractor shall provide RTD with a copy of the Contractor's privacy notice, privacy policy, and related documents as applicable to privacy governance.

C. Access Control. Two-factor authentication shall be used for anyone who has access to confidential and sensitive data from the Internet. Access shall be limited to only those individuals with a verified business need. Where feasible and applicable, role-based access control systems shall be implemented to enable user account administration by job role or function.

D. Logging. Record and/or field level access controls shall be implemented on all databases. Security audit logging shall be implemented for all confidential and sensitive data accesses. Contractor shall review the log files daily and report unauthorized access or suspicious activity to RTD as soon as possible.

E. Contractor's Access and Use of RTD Data. Without receipt of RTD's prior written consent, Contractor shall not: (i) access, process, or otherwise use RTD Data other than as necessary to facilitate the Work under this Contract; (ii) give any of its employees access to RTD Data except to the extent that such individual requires access to facilitate performance under this Contract; (iii) give any third party access to RTD Data, including without limitation Contractor's other customers, except for Contractor's subcontractors as set forth in subsection (E) below; and (iv) sell RTD Data to any third parties. Notwithstanding the foregoing, Contractor may disclose RTD Data as required by applicable law or by proper legal or governmental authority. Contractor shall give RTD prompt notice of any such legal or governmental demand and reasonably cooperate with RTD in any effort to seek a protective order or otherwise contest such required disclosure, at RTD's expense.

F. Risk Assessment. Contractor must perform a risk assessment prior to any major system change or installation that impacts the storage, collection, transmission or processing of RTD Data, including but not specifically limited to the addition of new systems, removal of systems, major upgrades, changes in data flows affecting RTD Data, or changes in security controls

related to RTD Data. Identified risks and mitigation plans must be reviewed with RTD prior to change implementation. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.

G. Privacy Impact Assessments. A privacy impact assessment must be performed for any major changes to the hosted systems that impact the storage, collection, transmission or processing of PII, to include addition of new systems, removal of systems, major upgrades, changes in data flows affecting PII, or changes in security controls related to PII. Mitigation for noted risks must be addressed in the change implementation plan. Risks that cannot be mitigated must be presented to RTD for review and acceptance prior to change implementation.

H. Ownership of RTD Data. RTD possesses and retains all rights, title, and interest in and to RTD Data, and Contractor's use and possession of RTD Data is solely on RTD's behalf as permitted by RTD. Contractor shall not withhold access from RTD to the RTD Data. RTD may access and copy any RTD Data in Contractor's possession at any time, at no cost to RTD. Contractor will facilitate such access and copying promptly after receiving RTD's request.

I. Open Records and E-Discovery. Contractor acknowledges that RTD Data may be subject to open records laws and e-discovery requests. In the event of an open records or e-discovery request applicable to the RTD Data in Contractor's possession, Contractor will cooperate with RTD, its subcontractors, and other third parties as necessary to preserve and produce the RTD Data. At RTD's request, Contractor will provide a copy of the RTD Data to RTD in a usable and readable, platform-agnostic format.

J. Encryption. Confidential and sensitive RTD Data stored in the system must be encrypted using strong encryption. Confidential and sensitive RTD Data transmitted across the Internet to or by the system must be protected by strong transport encryption. Contractor must use encryption key management strategies that are designed to prevent the corruption or exposure of encryption keys or abuse by individuals without a business need.

K. Vulnerability Scanning. All systems that store, collect, transmit, or process confidential and sensitive data that are accessible from the Internet shall undergo vulnerability scanning quarterly, with the results provided to RTD within one week of performing the scan. All high-risk defects must be corrected with scans re-performed to demonstrate defects no longer exist.

L. Data Retention. Only the least amount of confidential and sensitive RTD Data required to perform the Work and meet RTD's record retention requirements may be retained (whichever is more stringent). RTD shall communicate applicable data retention requirements to the Contractor prior to the collection of production data. Expired data shall be purged from all managed systems and applications upon expiration, or within a commercially reasonable timeframe following the expiration date not to exceed 30 days.

M. Retention and Deletion of Data. Contractor shall follow any commercially reasonable written instructions from RTD regarding retention and erasure of RTD Data, provided however that Contractor shall not retain any RTD Data beyond 30 days after termination of this Contract unless otherwise requested and approved by RTD. RTD Data shall be available to RTD to retrieve at any time and at no additional charge throughout the term of this Contract and for

no more than 30 days after expiration or termination of this Contract for any reason. Upon written request, promptly after destruction or erasure of RTD Data or any copy of RTD Data, Contractor shall certify such destruction or erasure to RTD in writing. In purging or erasing RTD Data as required by this Contract, Contractor shall leave no data recoverable on its computers or other media, to the maximum extent commercially feasible. All confidential and sensitive RTD Data shall be removed from systems by overwriting the media three times with 1s and 0s before disposal or transfer of assets outside of RTD's use or the Contractor's custodianship.

N. Data Replication. Contractor shall not duplicate confidential and sensitive RTD Data to other systems, including but not limited to test systems and databases, portable storage media, hard copies, or other locations where it is not necessary for the business or technical function of the Work.

O. Subcontractors. Contractor shall not permit any subcontractor to access RTD Data unless such subcontractor is subject to a written contract with Contractor agreeing to protect the data, with terms and conditions reasonably consistent with these terms and conditions. Contractor shall exercise reasonable efforts to ensure that each subcontractor complies with all of the terms of this Contract related to RTD Data.

P. Applicable Law. Contractor shall comply with all applicable laws and regulations governing the handling of RTD Data and shall not engage in any activity related to RTD Data that would place RTD in violation of any applicable law, regulation, government request, or judicial process.

Q. Data Breach. Contractor shall maintain the confidentiality of the RTD Data and exercise commercially reasonable efforts to prevent unauthorized exposure or disclosure of RTD Data. In the event of a data breach or unauthorized disclosure of RTD Data, Contractor shall (i) notify RTD's Contract Administrator by telephone and email within 24 hours of discovery of the breach or unauthorized disclosure; and (ii) cooperate with RTD and law enforcement agencies, where applicable, to investigate and resolve the matter, including without limitation notifying injured third parties. Contractor shall give RTD prompt access to such records related to a data breach or unauthorized disclosure as RTD may reasonably request, provided that Contractor shall not be required to provide RTD with records belonging to, or compromising the security of, Contractor's other customers. In the event of a data breach or unauthorized disclosure caused by the act or omission of the Contractor or any of its agents, employees, or subcontractors, the Contractor shall pay or reimburse RTD for any costs incurred with respect to: (i) notification to all affected individuals; (ii) repayment of lost funds; (iii) repair of damaged credit; (iv) one year of credit monitoring for all affected individuals; and (v) any other penalties and fines related to the breach or unauthorized disclosure.

R. Disaster Recovery and Business Continuity. Contractor shall maintain and implement a disaster recovery plan and business continuity plan to ensure the continuity of the Work provided to RTD pursuant to this Contract and the recovery of data or functionality lost due to operator error, system error, or other unforeseen circumstances and to ensure that the Work is not interrupted during a disaster or force majeure event. During the term of this Contract, Contractor shall provide RTD with a copy of its current disaster recovery and business continuity plans and all updates to these plans. Upon RTD's written request,

Contractor will issue to RTD a summary statement on the design of the business continuity management framework. The business continuity plan is confidential, and Contractor will not provide actual plans nor will it allow customers to participate in business continuity activities.

S. Location of RTD Data. Contractor shall not transfer RTD Data outside the United States without RTD's prior written consent.

T. Multi-Tenancy Servers. Should RTD Data be processed or stored on multi-tenancy servers, security controls shall be in place to ensure that a tenant with weak security settings cannot affect or interfere with the security of RTD Data as well as to ensure that data is not co-mingled within the server or stack.

U. Safeguards. The Contractor shall not publish or disclose in any manner the details of any safeguards designed to protect RTD Data without the prior consent of RTD.

CONTROL ACTIVITIES

At RTD's request, Contractor shall provide RTD the opportunity to review the design and execution of the control activities performed by the Contractor as it relates to the support and security of RTD's operations and the data, systems, networks, or facilities that are relevant to providing Work to RTD (as applicable to the Scope of Work).

ON-PREMISES SYSTEMS

Should the Contractor require the installation of an on-premises system to support the Work, either (a) at a minimum, RTD must have read-only administrative access to the system to verify security controls, or (b) the system must be separated from the RTD internal network using, at a minimum, logical access controls to restrict the system to the least necessary access to perform Work under the Contract. Any system placed on the RTD network must be capable of conforming to RTD's security policies and standards and architectural standards, including but not specifically limited to the following requirements: must have a supported operating system or firmware version; must be patched or updated to close security vulnerabilities; must support access controls that maintain user least-privilege; must be able to undergo configuration hardening; must be capable of running antimalware software (endpoints only).

WARRANTY

A. Contractor expressly warrants that the Product(s) will function and perform materially in accordance with the specifications as set forth in the Scope of Work for a period of 24 months following Final Acceptance by RTD.

B. For any software application or operating system Product, Contractor expressly warrants that the Product complies with Subpart 1194.21 of Section 508 of The Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990.

C. For any website Product, Contractor expressly warrants that the Product complies with Subpart 1194.22 of Section 508 of The Rehabilitation Act of 1973; Level AA of the Web

Content Accessibility Guidelines 2.1 of the World Wide Web Consortium (W3C) Web Accessibility Initiative; and the Americans with Disabilities Act of 1990.

D. In the event of a breach of the warranties above, Contractor shall promptly correct and repair any deficiencies in the Product(s) to the reasonable satisfaction of RTD, at the Contractor's sole expense. If the Contractor is unable to correct or repair the deficiency to the reasonable satisfaction of RTD, then the Contractor will refund RTD as follows: (i) if within the first 12 months of the warranty period, then all amounts paid by RTD for the Product(s); or (ii) if after the first 12 months of the warranty period, then 50% of the license fee paid for the Product(s) for every month remaining on the licensed term. If RTD does not require the Contractor to correct or repair the deficiency, then RTD will make an equitable adjustment in the Contract Cost.

RELEASE AND CHANGE MANAGEMENT PROCESS

A. Non-emergency change/release requests for test environments/user acceptance testing environments/production environments shall be submitted 10 calendar days in advance and shall be reviewed and, if found acceptable, approved in the monthly CAB (Change Advisory Board). The CAB consists of the RTD CIO, IT Managers, IT Service Delivery Team, and the Contractor.

B. Prior to installing into testing environments and user acceptance testing environments, Contractor must provide test scripts, test results and risk analysis, release notes, data flow, and process flow related to the particular change.

C. Emergency change/release requests for production must be submitted as soon as possible prior to release. RTD shall review and if found acceptable approve PROD deployment after convening an eCAB (Emergency Change Advisory Board). The eCAB shall be held as soon as possible after receipt of the emergency change/release request.

D. All releases for test environments/user acceptance testing environments/production environments shall require infrastructure/application documentation (i.e., data flow and process flow), risk or impact analysis for the affected application(s), test plan including type of testing to be performed, installation/release plan, and back-out plan.

E. RTD shall review and, if found acceptable, approve all results prior to a release moving forward to the next test environments/user acceptance testing environments/production environments.

F. RTD utilizes a number of tools/processes in regards to the Release and Change Management Process, and the Contractor shall utilize such tools/processes as needed and instructed by the Release/Change Manager.

G. For Contractor-hosted application and systems, RTD shall be provided access into the Contractor test environments/user acceptance testing environments/production environments to evaluate, test, and accept projects prior to production deployment of the applications and systems for RTD.

H. Changes that affect RTD's ability to conduct business will go through RTD's change process. Non-emergency change and release requests shall be submitted 10 calendar days in advance. Requests shall be reviewed and must be approved by the CAB.

I. The Contractor shall notify RTD in writing before commencing any Work on internal/external hardware, software, or business process changes that will affect RTD's ability to conduct business prior to the initiation. RTD shall review and, if found acceptable, approve any of the aforementioned changes before the change commences. This shall allow RTD to plan, review, and implement the necessary internal/external changes to accommodate the Contractor's requested change prior to implementation.

J. RTD must be notified in writing of any changes impacting outsourced services provided to the Contractor by third party vendors, when such changes could affect RTD's ability to conduct business.

K. RTD shall provide individual Contractor employees with remote and unique access to the environments for auditing purposes if deemed necessary for the Work.

L. The Release/Change Manager shall be the point of contact for RTD in regards to all change and release management activities.

ADDITIONAL RTD POLICIES

The following additional RTD policies are incorporated as attached:

A. RTD Management Directive dated 4/12/2016: Secure Computing Policy
B. RTD-CYBER-VR-05: Commercial Product Purchases Vendor Requirements
C. RTD-CYBER-VR-10: Network Access Vendor Requirements
D. RTD-IT-PLY-0001: Acceptable Use of RTD Technology Policy
E. RTD-IT-PLY-0002: Computer System and Network Configuration Policy
F. RTD-IT-PLY-0003: Electronic Data Protection Policy
G. RTD-IT-PLY-0004: Computer System Activity Logging and Monitoring Policy
H. RTD-IT-PLY-0005: Computer System and Electronic Data Access Control Policy
I. RTD-IT-PLY-0006: Information Technology Risk Management Policy
J. RTD-IT-PLY-0008: Cybersecurity Incident Response Policy
K. RTD-IT-PLY-0009: Secure Application Acquisition and Development Policy
L. RTD-IT-PLY-0019: Vendor Cybersecurity Management Policy

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

A. RTD Management Directive dated 4/12/2016: Secure Computing Policy

RTD

MANAGEMENT DIRECTIVE

Subject: Secure Computing Policy

Responsible Department: Finance & Administration
Effective Date: 4/12/2016
Approved by:

PURPOSE

Information technology, or IT, is a key component of almost all RTD processes. Ensuring that our information systems are available to support District business and the information that they collect, transmit, process, or store remains intact and secure is a necessary part of fulfilling the District's mission.

The Secure Computing Policy is designed to establish and maintain a secure computing environment and consistent, enforceable security practices for RTD employees and contractors in order to ensure RTD-owned and controlled information technology systems and data remain secure.

SCOPE

Everyone who uses information technology resources at RTD or technology owned by RTD is required to follow this policy, including employees, board members, and vendors, partners, and contractors.

To a limited extent, this policy also pertains to the use of technology equipment or resources that are not owned by RTD that you may choose to use at work where it is permitted by this policy, such as your personal computer, tablet, phone, drives, or other devices you may own and bring from home.

This policy is tailored for general computer users. Should you have responsibility for the deployment, administration, maintenance, and/or development of technology systems for the District, or should you work with or manage contractors with responsibility for those functions, please additionally refer to the **IT Security Policy for Enterprise Systems**.

DEFINITIONS

Contractors means people that work for another company, but who are doing work on behalf of or in conjunction with RTD, such as vendors, partner organizations. The Board

of Directors are considered contractors for the purposes of this policy insofar as Director services are mediated by an RTD employee delegate.

Employees means people who are directly employed by RTD.

Owner or "business owner" means a person, usually a manager, who is assigned primary responsibility for a piece of equipment or for the performance of a business process and the necessary technology and information stores required to make that business process work. Business owners may delegate administrative functions to their staff (such as managing access to the department's shared drives).

Manager means any person who has managerial responsibility for others (i.e. direct reports) within RTD. For the purposes of this document, "manager" is used generically and can refer to a supervisor, manager, senior manager, assistant general manager, or general manager, but typically refers to the person to whom you report directly.

RTD Information Technology or "RTD IT" means the RTD department that is assigned to deploy, administer, and maintain RTD information technology resources for the District.

RTD information technology resources include, but are not limited to desktop and laptop computers, tablets, enterprise systems (servers, network devices), wired and wireless network connections, RTD-owned software whether purchased or developed, RTD data stores and databases, portable media such as disks, tapes, or USB drives of any size, office phones and cell phones, radios, and other related peripheral equipment that is provided to you for RTD business purposes.

Service Desk means the RTD IT department that helps computer users report computer issues and assigns the issues to RTD IT personnel for resolution. Issues can be reported to the Service Desk by clicking the "IT Service Desk" link at the top of the Hub home page. All references to the Service Desk are linked to the online request submission tool. The Service Desk can also be reached by calling 303.299.6100.

POLICY REQUIREMENTS FOR EMPLOYEES

Access to RTD Computer Systems

Before accessing RTD computer systems and areas where IT equipment is accessible, you must request a unique identifier (most commonly a user ID, but can also be a badge, code, token, app, or other means of access) by submitting a Service Desk ticket to the IT department. If you are a manager of a new employee, you may request access for your employee to start on or after the employee's hire date by submitting a Service Desk ticket.

All access requests must be accompanied by the following:

- Business justification for the access

- Your manager's approval (or approval of the manager of the person for whom access is requested, if not you)

For shared systems, services, or applications, prior to granting access, the Service Desk will additionally request review and approval from the business owner of the system (i.e., the person responsible for the primary business functions performed by the system you want to access) prior to granting you access.

If you fail to provide a business justification and/or your access is not approved by your manager and the business owner (as applicable), your request for access will be rejected.

Exception: Access to departmental resources does not have to be processed by the Service Desk and can be administered by the owner of the resource. Examples include departmental shared folders and files, SharePoint sites, sections or views within a document repository, and test sites/test systems where only non-production data is stored or processed. Should you be a resource owner that chooses to use this model, you are responsible to periodically validate that only users with a business need for access retain ongoing access to your resources.

Only the minimum amount of access required to accomplish the stated business goals (within the justification) is granted. Managers are responsible to notify the Service Desk when there are changes in an employee's status or job role, for example when they change jobs or leave the business, so that access can be modified or terminated as appropriate. The Service Desk will provide you with direction on any additional actions you may need to take, such as providing an access delegate, in order to facilitate access changes and preserve business processes.

Periodically, IT will review system access for currency and validity, and may ask managers to update or confirm their employees' business justification for access. Should the manager fail to provide positive confirmation of his or her employees' access, the access will be terminated. Similarly, should you fail to login to your account for over 90 days, your access could be suspended.

Shared accounts, or accounts for which more than one person knows the user ID and password, are not allowed. Shared accounts that are required for systems management purposes must be reviewed, approved, and managed by IT. Other shared accounts currently in use will be phased out.

Access may be terminated at any time, without notice, by RTD IT if your computer or computing practices consistently violate the Secure Computing Policy or otherwise threaten RTD security or network integrity to protect and preserve computing resources for other users.

Appropriate Use of Technology Resources

You are allowed and encouraged to use RTD's computing systems and network, as requested and provisioned for your use, as necessary for business purposes and in a manner consistent with the District's standards for business conduct.

Never use RTD computer equipment or networks to engage in, download, access, or disseminate the following:

- Profane, vulgar, abusive or sexual language or content, or links to such content;
- Endorsements, contributions or promotion of political parties, candidates, groups or ballot measures except as allowed by RTD policies;
- Content that promotes, fosters, or perpetuates discrimination prohibited by law or RTD policies;
- Solicitation or endorsement of commercial products, services or entities;
- Conduct or encouragement of illegal activity;
- Uploading, downloading, or otherwise transmitting commercial software or copyrighted material in violation of its copyright;
- Intentionally interfering with normal operation and integrity of the network and/or RTD data for any purpose other than those specifically defined and authorized by RTD IT and senior management;
- Revealing or publicizing RTD confidential information;
- Information that may tend to compromise the safety or security of the public or public systems, including imminent threats, fighting words, or specific threats of serious bodily injury;
- Network and system security reconnaissance or "hacking" of RTD's or another company's systems (except in special cases authorized by the RTD IT security team for security testing purposes);
- Activity that is otherwise in conflict with the RTD Code of Ethics or Employee Guidelines (see Workforce Guidelines).

Social media is an important part of how RTD does business. The forthcoming Social Media Guidelines will provide more specific guidance for your use of social media.

Your use of RTD's computer resources may be monitored at any time, for any reason, by RTD IT at the request of management. Your privilege of using RTD's computer resources can be revoked at the request of management or by RTD IT if it represents a violation of policy or an imminent threat to the integrity of RTD's computing environment (*see also Privacy and Monitoring*).

Equipment Assignment and Tracking

Should you require or request a computer or telephony equipment (for example, desktop or laptop computers, tablets, desk phones, cell phones, smart phones, monitors, keyboards, mice, printers, USB drives or sticks, radios, card readers, and other devices) to complete your assigned responsibilities, you must request the equipment by submitting a Service Desk request. If you are a manager of a new employee, you may request equipment for

your employee to start on or after the employee's hire date by submitting a Service Desk ticket.

All computing and telephony equipment assigned to you by RTD remains property of RTD. You are responsible to physically secure the equipment against theft or misuse (*see also Equipment Security*) and return it to RTD IT when no longer needed or at the end of your employment. In the event that your computing or telephony equipment breaks or becomes unusable, submit a Service Desk request to have the equipment repaired or replaced; do not "shelve" the equipment, dispose of the equipment, or attempt to fix it on your own.

Some computing and telephony equipment is specifically assigned to you and is only for your use, either because it is considered an attractive asset (see also Accountability for RTD Equipment Management Directive) or because its use and management is directly tied to your name, location, login, or data on the device. Examples include, but are not limited to, your computer, tablet, cell phone or smart phone, or desk phone. If you no longer need the equipment or want to transfer it to another user, submit a Service Desk ticket so that RTD IT can properly re-deploy the equipment. Computer peripherals and other low-value items such as keyboards and mice do not require a Service Desk ticket to move or exchange with another RTD user.

Managers are assigned and responsible for equipment that is shared among members of their department. Managers must track who uses their shared equipment and establish protocols for how the equipment is checked out, checked in, and stored in the interim (*see also Equipment Security*). If you use shared equipment during the course of your job, you are responsible to abide by the requirements of this policy for the period in which the equipment is in your use and possession, and you are responsible to return the equipment to the manager-designated storage location when you are finished using it.

RTD IT may use passive scanning software to identify computers and computer equipment on the network for inventory and management purposes. You may not block or uninstall components that facilitate equipment update and inventory for any reason. If you feel that one of these functions is causing a problem, please call the Service Desk for assistance before taking any action on your own.

Equipment Security

You are responsible to physically secure all computer and telephony equipment assigned to you against loss and theft. Inside of RTD, your computer, phone, and other equipment assigned to you must be installed or stored in an internal area where access to the area is controlled and/or monitored by RTD Security. It is recommended, although not required, that you store all small portable equipment – especially that which contains data – in locked offices, cabinets, or drawers when you are away from the office to deter incidental theft. You may not otherwise leave your computer or other equipment unsecured and unattended in areas that are not considered and secured as "internal" areas and are

generally accessible to the public (for example, in an office lobby or bus station), even if it is on RTD property.

Managers whose staff share equipment must ensure that only authorized employees have access to the equipment and that the equipment is stored in a safe location, such as a locked cage, cabinet, vault, or other RTD-controlled secure area when not in use. Managers must periodically inventory all assigned equipment to identify instances of loss or theft.

If you are required to take RTD equipment off premises, the following rules apply:

- Do not put any devices that store or access RTD information in checked baggage (or equivalent) while traveling.
- Keep all portable devices within reach while using public transportation.
- Do not leave your computer equipment for long periods of time in an unattended vehicle. If you must leave your computer, phone, smart phone, or tablet in a vehicle, stow the device(s) where they are out of sight and locked up, for example in the vehicle trunk or glove box.
- Protect handheld assets, such as a smart phone or USB stick, as you would a wallet.
- When staying in a hotel, lock all portable computing equipment in the hotel safe while you are out of your room. If there is no hotel safe available, either take the devices with you, or tether the device to a secure surface with a cable lock (available by submitting a Service Desk request).
- Do not leave your computer, phone, or other devices unattended in public areas, such as in coffee shops or at conferences.
- When working with RTD confidential information, be aware of others in your vicinity and protect the information displayed from others' view or choose a more appropriate work location.

The value of the data on a computer, smart phone, tablet, or other device could far exceed the monetary value of the equipment itself. If your equipment is lost or stolen, and it also stores data (example: a computer, smart phone, tablet) or is otherwise considered an attractive asset (see also Accountability for RTD Equipment Management Directive), you must immediately report the incident to the Service Desk and the Transit Police (see also Theft Response Management Directive).

File Sharing and Collaboration

RTD makes several internal resources available to you for information sharing and collaboration, including internal email, the Hub (SharePoint), shared drives (N:, P:, others), and document management software (Aconex, Documentum). Should the existing information sharing and collaboration tools not meet your business needs, submit a ticket to the Service Desk to request a solution. Do not attempt to purchase, install, or sign up for file sharing software or services without first consulting the Service Desk (*see also*

Software Installation and Use). Should you choose to install or sign up for file sharing services without prior Service Desk review or engage with services that otherwise represent a security risk to RTD, they may be uninstalled or blocked by RTD IT.

If you are working with sensitive information, you must abide by this policy's requirements regarding the handling of sensitive information. You are responsible to identify whether the information you are working with is sensitive and apply or ensure the appropriate security controls are applied according to this policy (*see Sensitive Information*).

Regardless of the sensitivity of the data being shared, never install or use peer-to-peer file sharing software or torrent sites (for example, but not limited to BitTorrent) on or while connected to RTD technology equipment.

Guests and Visitors

Guests, meaning visitors who are invited by RTD to conduct business or visit an employee at the RTD facilities, must complete the Security check-in process for visitors at each RTD facility.

RTD provides wireless Internet access for RTD guests. RTD guest networks may also be used by employees or contractors that would like to access the Internet strictly for non-business purposes (for example, to check personal email). RTD guest Internet access is not designed to support or intended for use by members of the general public.

The guest network name (SSID) and password may be posted in RTD conference rooms out of sight of areas frequented by the general public (for example, front doors, windows, and lobbies). Do not share or post the RTD guest wireless password outside of RTD's facilities, or within sight of RTD public areas.

Logon, Logoff, and Locking Your System

The following requirements are designed to protect you and RTD from unauthorized people accessing your computer resources and sensitive data when your computer, phone, smart phone, or tablet is unattended:

- You must login (ex. provide your user ID and password) to prove your identity every time you access your computer. You may not configure your computer to login automatically.

Exception: Shared computers are exempt from this requirement in approved configurations administered by RTD IT.

- You must log out of your systems or activate a password-protected screen lock that is activated after 15 minutes of inactivity.
- When leaving your work area, you must activate your password protected screen lock (for Windows systems, the lock command is "Windows Key + L"; on Mac systems, the lock command is "Apple Key + L"). For tablets and smart phones,

activate the password protected screen lock when you are finished using your device (ex. using the Sleep key).

- Should you fail to login to your computer more than six times, your account will be locked out for at least 30 minutes, or until it is re-enabled by an administrator. If you accidentally lock your account, please notify the Service Desk to unlock your account or to perform a password reset (*see also Passwords*).

Never allow another person to use your computer while it is logged in as you and then walk away. Anything that person does on your computer not only traces back to your ID, but is limited only by the rights and permissions assigned to your ID. If there is a business need for someone to use your computer while logged in as you, you must actively monitor their activities. If you need to let someone else use your computer while you are not present, you must log out of your computer and let the other person log in with their own ID.

Network Access - Onsite

RTD provides wired and wireless connections for your use at work. Network ports and wireless access must only be configured by IT. Should you need a network port installed or activated or require assistance with wireless access, please contact the Service Desk. You may never install personal or RTD-purchased equipment that extends the RTD network, for example wireless routers plugged into your office or a conference room LAN port, without intervention and approval by IT. Discovery of unauthorized equipment constitutes a security incident.

Network Access - Remote

Anyone with general RTD network access may access resources such as email, Oracle E-Business Suite, and basic business applications remotely using the RTD Citrix web portal, https://myportal.rtd-denver.com. The Hub (SharePoint sites) can be similarly accessed across the Internet using your network access login.

Virtual Private Network (VPN) access is only granted to employees under the following circumstances:

- You need to work remotely more than 30% of the time
- You have a justifiable business need for access to a service or application during an emergency or after hours that is not available as a Citrix published application

Office Moves

Changing office locations involves a lot more than moving the physical computer or phone. Do not attempt to move on your own; always submit a ticket to the Service Desk to request an IT equipment and services move. IT can update your tracked equipment locations, change and activate your phone and network connections, and assist with physically moving the IT equipment to your new location and ensuring it is connected and working properly following the move.

Passwords

Passwords, access codes, physical access keys, badges, and other authentication keys are confidential to each individual. **You may never, under any circumstance, share your password, badge, access codes, or equivalent with anyone, inside or outside of RTD.** Attempts to circumvent this requirement by logging in and leaving your computer in someone else's control without your presence or allowing someone to use your badge to access facilities is considered equivalent to password sharing and is a violation of this requirement.

Regardless of whether the following is enforced by the IT system, your password must meet the following requirements:

- Must be at least 8 characters in length
- Cannot contain any part of your name or user ID
- Must contain at least one uppercase letter, one lower case letter, one number, and one special character (ex. ! @ # % $ ^ & * - _)
- Must be changed at least every 90 days

Never write down your password and store it so that others are apt to see it; this includes on the back of monitors, the inside of drawers, and under keyboards. Similarly, never store passwords inside of software programs that you use to access sensitive data so they can be used for automatic login (ex. "Remember Password" features). Should you be unable to remember your password, request a password reset from the Service Desk. Should you routinely have trouble remembering your passwords, the IT department can provide you with a secure password vault solution.

Shared accounts, or accounts for which more than one person knows the user ID and password, are not allowed to be used and will be phased out. Should you use a shared account in the interim or by exception, you must never publicly post the password.

Exception: Guest network access passwords may be posted in RTD conference rooms only to facilitate guest network access. See Guests and Visitors for the requirements surrounding guest access passwords.

If you know or suspect at any time that your password has been exposed, you must immediately change your password or request a password reset from the Service Desk. You must change first time or one time use passwords, such as those provided by the Service Desk, to a value other than what you were provided upon the first use.

Personally-Owned Devices Used at RTD

You may choose to use your personally owned devices, such as a computer, smart phone, or tablet, to conduct RTD business. Any information that you generate on behalf of RTD is RTD property, regardless of whether the information was created or stored on your personal device. You may choose to use your device offline (not connected to RTD's network) or online (connected to RTD's internal network). In either circumstance, if you

use your device to generate, store, process, or transfer RTD data, your device must meet RTD's security requirements per this policy.

You may not connect a personal device to RTD's network or other technology resources for solely personal / non-business purposes, such as to access the Internet to check personal email, play games, watch movies, or download music, unless you are connecting to the guest wireless connection for short-term use (*see Guests and Visitors*). Should you choose to connect your personal device to RTD's internal network for business purposes, then have a need to use the device or RTD's network connection for personal use, you are subject to the requirements in Personal Use of RTD Technology insofar as you are using RTD's network resources for personal business.

Note: It is your choice to use your personal device at RTD, but RTD's choice to manage RTD's technology resources you use and RTD's data that you access or store on your device. The following may impact your decision whether to use RTD-provided or personal equipment in the performance of your job duties:

- RTD IT will only provide support for those systems and services that are required to fulfill a business need.
- You must comply with all requirements of this policy that are not specifically applicable to RTD-owned equipment when using your personal device for RTD business purposes, including but not limited to System Configuration Security – Non-RTD Equipment. The policy requirements apply whether you are using the device on RTD property (in the office) or using your device to connect to RTD remotely (for example, via Citrix or VPN; *see also Network Access - Remote*). These may require that you purchase, install, and manage additional security software and regularly maintain your system.
- Lost or stolen RTD-owned or personal tablets or smart phones that are used to access RTD information, such as email, may be remotely wiped by RTD IT. This will result in the loss of all local data on the device.
- Your personal devices or data generated by your personal devices can be scanned and monitored insofar as they are used in conjunction with RTD data and technology under the Privacy and Monitoring requirements.
- RTD information generated on or stored in your personal device could be subject to discovery in a records management or legal investigation. Depending on the scope of the request, your personal information could be disclosed in the research and presentation of RTD-related information.

RTD IT will disconnect and ban personal devices from the network, at its discretion, if they are found to be out of compliance with this policy, represent a security risk to the network, or otherwise consume unnecessary technology resources.

Exception: Personal devices that are brought on premises but not used for RTD business or connected to the RTD internal (non-guest) network are not subject to the requirements of this policy.

Personal Use of RTD Technology

You may use RTD's technology resources (computers, phones, tablets, and other devices) for personal purposes provided that it is limited and brief in duration, does not interfere with the performance of your job duties, does not put undue stress on the network or systems owned by RTD, and does not interfere with the activities of other computer users. Examples of limited personal use include checking weather, checking personal email, making an emergency call from an RTD-issued cell phone, reading a general or business-related news website or blog, or checking a travel itinerary. Managers are responsible to communicate appropriate guidelines and thresholds for personal computer use to their employees that are based on their department's needs and responsibilities and to monitor their employees' use of RTD computing resources for compliance to established guidelines and thresholds.

You may not download, install, or store personal software (including apps) or an unreasonable number of personal files on your RTD-owned equipment or store any personal files on the RTD network unless required for business purposes. You may be asked to provide a business justification for software or files found to be present on RTD equipment. If you cannot provide a business justification, RTD IT will uninstall the software or delete the files.

You are responsible for additional fees or charges incurred, if any, while using RTD equipment for personal use, including air time and overage charges.

You are still required to abide by all requirements of this policy when using your RTD computer or other technology resources for personal use. Additionally, RTD IT may choose to set limits or access permissions on your (or the entire District's) access to non-business content or services to ensure that sufficient technology resources are available and accessible for business purposes and to enforce the appropriate use policy (*see Appropriate Use of Technology Resources*).

RTD IT does not provide support for technology functions unrelated to RTD business.

Phishing

Scammers may pose as legitimate companies or individuals to try to trick you into giving them money, sensitive information, or access to RTD's buildings, systems, or data (*see also Remote Control Software*). This is referred to as "phishing." Phishing can be done in person, over the phone, or over the computer (commonly through email or social media). You can learn how to identify phishing attempts by taking the Cybersecurity@RTD security awareness training on the Hub.

If you receive a phishing email:

- **Do not click any links and do not open any attachments;**
- **Do not forward the email to other users unless specifically directed by RTD IT;**
- Contact the Service Desk to describe the phishing email. You may copy the text of the phishing email into the Service Desk request. Should RTD IT require a copy of the email, the responding IT personnel will provide you with directions on how to provide the copy.

However unintentional, if you respond to a phishing scam, immediately report the incident to the Service Desk and describe what happened, how, and when. An IT risk investigator will be assigned to work with you to determine whether any harm has been done to your computer and formulate an appropriate response plan (*see also Security Incidents*).

Note: Unsolicited advertisements or bulk email that do not prompt you to take specific action are called "spam" and are handled differently (*see Spam*).

Privacy and Monitoring

Your use of RTD's technology resources constitutes your consent to be monitored, and you should have no expectation of privacy when using RTD's technology resources.

At the direction and under authority of RTD management, RTD IT may monitor, log, and review any and all activities in which you engage using RTD technology resources (for example, computers, networks, phones, email, web browsing) at any time, with or without your knowledge. Your manager, RTD Legal, or RTD IT's security team may obtain access to and copies of files from your RTD computer, your email, your home drive, your browsing history, and other data generated by or stored on your computer upon request and/or with approval from your manager or a more senior manager in your reporting chain, as appropriate, in order to obtain information necessary to continue RTD's operations, maintain compliance with RTD's or other governing policies, as requested by a court of law, or in response to an IT security investigation. Your personal devices or data generated by your personal devices may also be subject to inspection if you use them to conduct RTD business and/or in conjunction with RTD technology resources.

Should RTD IT become aware through our routine system monitoring processes that you are engaged in illegal activity or activity which is otherwise harmful to the District and its interests, RTD IT will inform your manager, your Assistant General Manager, the Transit Police, and local law enforcement, as appropriate.

Remote Control Software

Remote control software allows another user to have control of your keyboard and mouse as if they were sitting at your computer, but from across the network. You may use remote control software to view and administer computers that are under your own

administrative control (for example, your own assigned computer(s), or other systems for which you have direct administrative responsibility).

There are cases where another person may need to remotely control your computer, for example, when an IT person needs access to fix your computer in response to a service request. In cases where IT needs to access your computer in order to fix it, IT will inform you in advance, you must (and IT will ask you to) log out of your computer prior to IT taking remote control of your computer, and the support person will use his or her own ID to login and perform support functions on your computer.

Do not fall victim to scams: A common phishing technique is to call a computer user, claim to be from a major computer company, and coerce the computer user into allowing the caller to have remote access to their computer. **IT support is always initiated by the RTD IT Service Desk or Deskside support, and never by an outside / non-RTD party. If anyone else asks to fix, have access to, or provide information about your computer, and you are not sure if the request is valid or originating from RTD IT, please contact the Service Desk before taking any other action** (*see also Phishing*).

There are cases in which a known business need dictates that a non-IT user (for example, IT support, a services vendor, or a coworker) remotely control your computer while you are logged into it. This is equivalent to allowing someone else sit at your keyboard and "drive" your computer. In these circumstances, always plan for the need in advance, verify the identity of the user who is taking over your screen, and actively monitor the session while in progress, just as you would if the person were sitting at your desk. Never let your computer be remotely controlled while you are not present.

Screen Sharing Software

Many RTD departments use screen sharing software to collaborate with others. During screen sharing sessions that include external entities (for example, a web conference) where you are required to display a portion of your screen. Only display the materials that you are required to display to accomplish the business goal of the session (for example, do not share your whole desktop unless necessary). (*Some screen sharing software also incorporates remote control capabilities; see also Remote Control Software.*)

Security Incidents

Technology-related security incidents are:

- Events that negatively affect the security of RTD technology resources (computer systems or data);
- Can be real (self-evident) or suspected.

Examples of technology-related security incidents include, but are not limited to:

- A computer, phone, or other device that contains RTD information is lost or stolen;

- Sensitive information is purposely or accidentally viewed by someone who has no business need to see it;
- A computer system is infected, taken over, or changed without knowledge or permission of the owner and primary user of that computer system.

You must report all actual and potential security incidents immediately to your manager and the Service Desk. If you know or suspect that there is an imminent threat to passenger or employee safety, you must additionally report the incident to the Transit Police Security Command Center (303-299-2911). Theft of physical equipment must additionally be reported according to the Theft Response Management Directive (*see also Equipment Security*).

Unplugging, disconnecting, or otherwise locking or blocking connections to a device can immediately stop an active attack on RTD systems, however, these and other actions may have unexpected and major downstream effects on RTD's ability to provide service, inadvertently destroy evidence or information that is needed to investigate and fix the problem that led to the incident and/or prosecute the offender(s), and/or may threaten the completion of RTD business if you accidentally misinterpreted events within the normal course of business as a security incident. **If you have any doubt as to what to do under the circumstances, do not attempt to stop, further investigate, or take any other action with regard to the potential incident unless otherwise directed by the Transit Police and/or RTD IT. You can reach the Transit Police at 303.299.2911 and the IT Service Desk at 303.299.6100.**

Sensitive Information

Any information that may do harm to RTD or RTD's customers if it is exposed to individuals without a business need to know is considered "sensitive." Sensitive information may include, but is not limited to:

- RTD confidential and/or proprietary information: unreleased business plans and ongoing business dealings, human resources information, financial data, attorney-client privileged information;
- Personally Identifiable Information (PII): name, address, date of birth;
- Sensitive Personal Information (SPI): social security numbers, drivers' license numbers, bank account information, credit card numbers, health information;
- Security Sensitive Information (SSI): security plans, reports of security gaps or vulnerabilities;
- Access codes (including passwords).

Sensitive information may only be accessed and used by employees with a business need to know and work with the information. Never provide sensitive information to an individual inside or outside of RTD without verifying their authority to access the information.

Never leave hardcopy documents, CDs, disks, drives, or other media containing sensitive information in an area where they can be accessed by unauthorized individuals, such as on a printer tray or on your desk. Retrieve sensitive documents from the printer immediately, and store documents and media containing sensitive information in a locked drawer or cabinet. If you need to destroy a document or other media that contains sensitive information, you must use a crosscut shredder or an RTD IT-authorized disposal service. RTD technology resources that contain sensitive data can be returned to RTD IT for destruction or secure erase and repurposing by entering a Service Desk ticket to request an equipment pickup.

Inside of RTD, authority to access and work with information on computer systems is controlled through access requests (*see Access to RTD Computer Systems*). You are responsible to identify sensitive information that you work with in the normal course of business and apply or request RTD IT to apply access controls to restrict users without a business need to know from viewing or changing sensitive data. Never post sensitive data to an internal repository that is openly accessible to all RTD employees, such as a public area of the Hub or a public shared drive (for example, "P: drive").

RTD provides several secure internal resources for working collaboratively with sensitive information. Never post or copy sensitive information to public information repositories, data management tools, or services that are not under RTD's control, including your personal accounts. These include, but are not specifically limited to your personal email accounts (Gmail, Yahoo!), publicly available or personal data sharing sites or cloud drives (Google Drive, Dropbox, OneDrive, Sky Drive), instant messaging (Google Talk), or social media sites (Facebook). Take care when working with RTD and personal devices to ensure that sensitive information is not inadvertently backed up to your personal cloud drive or another publicly available service. While it is highly discouraged, if you have a business need to store or transfer sensitive information using a portable device such as a laptop, tablet, smart phone, or USB stick or drive, the information must be encrypted to prevent unintentional access if the device is lost or stolen.

If you are contacted by an outside party and requested to provide sensitive information about RTD, do not provide the information and contact the RTD Legal Department for further assistance. If you have a confirmed requirement to provide sensitive information to an outside party, you must encrypt the information so that it cannot be read by unauthorized individuals when transmitted across the Internet. If you do not have encryption software, you may contact the Service Desk for a solution.

RTD has specific policies for handling certain sensitive information types, such as Protected Health Information (PHI), which is subject to the Health Insurance Portability and Accountability Act (HIPAA), and credit cardholder data, which is subject to the Payment Card Industry Data Security Standard (PCI-DSS). Should you work with either of these data types as part of your job responsibilities, request a copy of the related policy from your management, review, and ensure your compliance with the additional policy.

You are obligated to report any unprotected sensitive information that you encounter or unexpected changes in access controls to the Service Desk (*see also Security Incidents*).

Consult the Employee Guidelines and the RTD Code of Ethics in the Workforce Guidelines section of the Hub for any updates which may supersede this policy and for the latest official definitions of RTD confidential and proprietary information.

Spam

Spam, junk email, or unsolicited bulk email or other advertisements, is/are automatically filtered by RTD's email system. Occasionally, spam may bypass the email filtering program and be passed through to your inbox.

If you receive spam email, do not click any links, and do not open any attachments. Delete it; no further action is necessary.

If you continue to receive spam, you may open a Service Desk request and describe the issue so that RTD IT can adjust the email filter strength and rules. Never forward spam to other personnel unless you are specifically asked to do so by the RTD IT personnel assisting with the spam issue.

Note: Unsolicited attempts to gain access or information from you are called "phishing" incidents and are handled differently (*see Phishing*).

Software Installation and Use

You must submit a ticket to the Service Desk to request new software be installed (purchased, downloaded, or otherwise acquired) on your computer. **Do not purchase, download, or otherwise acquire and install software on your computer without first consulting with the Service Desk to determine whether a licensed and/or preferred product is already available.**

If you are authorized through the Service Desk to purchase and/or download software, the following rules apply:

- Only install validly licensed products for commercial or government use, and not products that are pirated, cracked, for educational or personal use only, or otherwise invalidated for commercial or government use.
- Do not install personally-owned software or software intended solely for personal use, including productivity software, apps, or games, on RTD-owned equipment.
- Do not install mobile applications from unofficial app stores or other untrusted sources (for example, you may install Android applications from the Google Play store, but not from an unofficial / other source).
- When installing applications on a tablet or smart phone, only permit access to the functions that the application requires in order to operate.
- You may not install RTD-owned software on non-RTD equipment.

Should you choose to install software without prior RTD IT review or software that otherwise represents a security risk to RTD, it may be uninstalled or blocked by RTD IT.

System Configuration Security – RTD Equipment

Your computer and other technology devices provided by RTD IT comes pre-configured to an RTD-approved security baseline and includes security software packages, such as antivirus and a personal firewall. You may not change, uninstall, or turn off any of the security features on your computer, at any time, for any reason.

Periodically, RTD IT must update your computer to ensure that it has the latest security settings and patches. RTD IT will notify you when such an update is required. You must comply with all of the requirements of the update process, including rebooting your computer if required. Do not intentionally circumvent the update process. Intentionally circumventing the update process constitutes a violation of this policy. If necessary, RTD IT will assist with manually updating your computer.

If you have questions about the security settings and software on your computer, you may submit a ticket to the Service Desk and IT will address your concerns.

System Configuration Security – Non-RTD Equipment

Computers or related technology that you own and choose to use for work under the Personally-Owned Devices Used at RTD policy must meet the following basic security requirements, insofar as these requirements are applicable to the specific type of device you are using:

- You must be running a fully operational, fully licensed antivirus product that provides real-time protection and blocks harmful code, checks for product and signature updates daily, scans your device periodically, and generates logs for review.
- You must be running a fully operational, fully licensed personal firewall product that detects trusted and untrusted networks, denies access from unauthorized systems, remains up to date with the latest product version, and alerts you to new programs requesting network access.
- You must be running an operating system version that is still supported by the software manufacturer.
- You must periodically install security updates to your device or enable automatic updating of your device.
- You must configure your computer, tablet, or smart phone to request a password upon login.
- You may not use a smart phone or tablet that is "rooted" or "jailbroken" to work (meaning, you have used software hacks to obtain elevated control over the management of your device's operating system).

Should you have questions regarding whether a specific software satisfies the requirements, what kind of software you should install to meet the requirements, or how to configure your computer to meet the requirements, please contact the Service Desk.

Training

All RTD salaried employees are required to take RTD's computer security awareness training, Cybersecurity@RTD, within 30 days of the start of employment and at least once per calendar year thereafter. Security awareness training is distributed and tracked by RTD Education and completion of such, or lack therein, is a permanent part of salaried employees' employee record.

Represented employees are encouraged to participate in the training. Represented employee participation is not tracked or reported.

POLICY REQUIREMENTS FOR SUPERVISORS OF CONTRACTED STAFF

The following policy requirements and clarifications apply if you are a supervisor of contracted staff – such as vendors or consultants – who use RTD's IT resources or access areas where IT equipment is accessible. You are a supervisor of contracted staff if you are an RTD employee providing management oversight and work direction to a vendor, partner, or contractor.

Access to RTD Computer Systems

Before allowing your contractor to access RTD computer systems and areas where IT equipment is accessible, you must request a unique identifier (most commonly a user ID, but can also be a badge, code, token, app, or other means of access) on behalf of the contractor by submitting a Service Desk ticket to the IT department. Note: Unique identifiers must be individually assigned and cannot be shared among a group of contractors.

The unique identifier for your contractor(s) is linked by IT to your employee ID. You are responsible to communicate changes in access needs to the IT department via Service Desk ticket, including the need to terminate access when the contractor's term expires, or to suspend access between contract terms or during extended absences.

If longer term facilities access is not needed, you may escort your contractor to and through areas where IT equipment is stored as a visitor. You must ensure the contractor completes the Security check-in process for visitors at the facility. If your contractor does not have and wear the visitor's sticker provided by Security, he or she will be denied access to the IT area (*see also Guests and Visitors*).

Employees requesting access on behalf of contractors must abide by the same authorization requirements as employees, where you as the contractor supervisor act as the approving manager, and contractors using the access are subject to the same reviews and restrictions as employees.

Appropriate Use of Technology Resources

Contractors must abide by the same Internet use requirements and restrictions as employees when using RTD equipment or network resources (ex. Internet connection).

Equipment Assignment and Tracking

Supervisors of contracted staff are assigned and accountable for all RTD computing and telephony equipment that is assigned to their contractor(s). Contractors must otherwise comply with the same requirements as employees regarding equipment assignment and tracking.

Equipment Security

Contractors must comply with the same requirements as employees regarding equipment security, where equipment is assigned to them by RTD.

File Sharing and Collaboration

Contractors must comply with the same requirements as employees regarding files sharing and collaboration where RTD information is being exchanged.

Supervisors of contracted personnel are required to identify whether the contractor will encounter sensitive data in the course of business and to ensure the policy requirements for sensitive information are followed (*see also Sensitive Information*).

Guests and Visitors

Contractors may not bring guests of their own to RTD without prior notification to and authorization from the supervising RTD employee.

Contractors that are not individually badged may be considered guests and complete the appropriate guest access procedures on accessing RTD facilities that house RTD IT equipment.

Contractors must otherwise comply with the same requirements as employees regarding guest and visitor access.

Logon, Logoff, and Locking Your System

Contractors must abide by the same logon, logoff, and lock requirements as employees.

Network Access - Onsite

Contractors must abide by the same network access requirements as employees.

Network Access - Remote

Contractors may use the same remote access resources as RTD employees, provided that it is required to complete their duties as assigned and sponsored by an RTD employee (*see also Access to RTD Computer Systems*).

Additionally, Virtual Private Network (VPN) access may be granted to contractors who require VPN access to perform the duties of their job per their agreement with RTD.

All contractor access established for non-general business purposes must be facilitated by IT and governed by the terms of the agreement with RTD. Examples include access for the purpose of data consumption or download, access to the RTD internal network for support purposes, and other business-to-business connections. Such connections are typically established within the scope of a project, but if initiation of a connection is required, please contact the Service Desk.

Office Moves

Supervisors of contractors must request office move assistance on behalf of their contractors by submitting a Service Desk ticket. Contractors may not request their own office moves; such moves must be sponsored by the supervising RTD employee.

Passwords

Contractors must abide by the same requirements as employees in their use and management of passwords.

Personally-Owned Devices Used at RTD

Contractors must abide by the same requirements as employees where contractors are using their own or their company's equipment in the RTD environment under the Personally-Owned Devices Used at RTD policy.

Personal Use of RTD Technology

Contractors are prohibited from storing personal files on RTD equipment and networks. Contractors must otherwise abide by the same requirements as employees regarding personal use of RTD technology resources.

Phishing

Contractors using RTD computing resources are subject to the same requirements and restrictions as employees regarding phishing when RTD technology is used as a delivery method for the phishing attempt. Contractors may report issues to the supervising RTD employee, who in turn is responsible to provide the appropriate guidance per this policy and/or engage the Service Desk.

Privacy and Monitoring

Contractors using RTD computing resources are subject to the same privacy and monitoring policies as RTD employees.

Remote Control Software

Contractors must abide by the same requirements as employees where RTD equipment, services, or data is involved.

Screen Sharing Software

Contractors must abide by the same requirements as employees where RTD equipment, services, or data is involved.

Security Incidents

Contractors must abide by the same requirements as employees where security incidents are concerned. Contractors may report security incidents to their supervising RTD employee, who in turn is responsible to report the incident to the Service Desk and the Transit Police Security Command Center.

Sensitive Information

Contractors are required to sign a non-disclosure agreement with RTD prior to commencing work that brings them into contact with RTD sensitive information. The supervisor of the contracted personnel can request a copy of the non-disclosure agreement form and processing instructions from RTD Materials Management.

Note: The RTD Board of Directors signs the RTD Code of Ethics in lieu of a separate non-disclosure agreement.

The supervisor of the contracted personnel is responsible to determine work with the owners, creators, or managers of information with which the contractors will come into contact to determine whether the information is sensitive, whether the contractors need access to the sensitive information to complete their work or can be excluded from access, and the appropriate level(s) of access control.

Contractors that work with RTD sensitive information must otherwise abide by the same requirements as employees.

Software Installation and Use

Contractors must abide by the same requirements as employees regarding software installation and use. Contractors may be allowed to install RTD-owned software on their company or personal device that they use to conduct business for or on behalf of RTD where specifically required by the terms of their contract or agreement with RTD and if they are not otherwise provided RTD equipment on which to install the software. Contractors are required to remove the software provided by RTD at the end of their tenure with RTD.

Spam

Contractors using RTD computing resources are subject to the same requirements and restrictions as employees regarding spam when RTD technology is used as a delivery method for the spam. Contractors may report issues to the supervising RTD employee, who in turn is responsible to provide the appropriate guidance per this policy and/or engage the Service Desk.

System Configuration Security – RTD Equipment

Contractors must abide by the same requirements as employees where RTD equipment is assigned to the contractor.

System Configuration Security – Non-RTD Equipment

Contractors must abide by the same requirements as employees where contractors are using their own or their company's equipment in the RTD environment under the Personally-Owned Devices Used at RTD policy.

Training

Contractors are encouraged to participate in Cybersecurity@RTD training at least annually. Contractor participation is not tracked or reported.

RESPONSIBILITY & ENFORCEMENT

All personnel with individual computer access must read this policy and sign to certify their receipt and understanding of the policy before they will be provided with any RTD computer access or equipment.

Devices that do not meet the policy are considered a security risk and can be removed from the RTD network. RTD IT reserves the right to determine whether you are meeting the policy and whether your use of technology represents a security risk to RTD, and to what degree.

Should RTD IT become aware that you are not compliant with this policy, RTD IT will take the following actions ("three strikes"):

- For routine or low-risk compliance situations, first offense, RTD IT will notify you that you are not compliant and request that you make corrective actions within one business day.
- For routine or low-risk compliance situations, second offense within 30 days of the last offense on the same topic, RTD IT will send another request for you to make corrective actions within one business day and copy your manager on the request.
- For routine or low-risk compliance situations, third offense within in 30 days of the last offense on the same topic, OR for high-risk situations, RTD IT will revoke your network access and notify your manager of the reason your access was revoked. You will need to provide proof of corrective actions taken and request your account to be reactivated by the Service Desk.

RTD IT can provide you with information and assistance on solving security and compliance problems and will provide direct support for your RTD technology equipment. In some circumstances, corrective action may consist of or include re-reading the policy or re-training to ensure that you don't repeat certain behaviors that violate the policy

(example: password sharing). If you need help making your technology equipment comply with the requirements of this policy, please contact the Service Desk.

There may be circumstances in which a temporary exception from the security policy is appropriate. It is your responsibility to provide a business justification for the exception, and RTD IT's responsibility to audit the exception request and business justification to see if we can resolve the problem. If the problem related to the exception cannot be resolved in a timely fashion, RTD IT will record the exception, the business justification for the exception, the scope of the exception (users for which it is valid, for example), what it would take to resolve the exception, and RTD IT management approval of the exception. RTD IT will additionally seek approval from the senior manager of the business unit for exceptions that represent a high risk to the District. RTD IT will periodically review exceptions to determine whether they can be resolved with new configurations or technology as District capabilities change.

DOCUMENT CONTROL

Document Availability

This document is available on the Hub, on the Workforce Guidelines site, within the Management Directives section.

Changes to This Document

This document is reviewed at least annually and following any major environment change. RTD Senior Management otherwise reserves the right to amend the policy at its discretion to meet District needs. You will be informed when an updated policy version is published and asked to review the policy and/or complete training, as appropriate. Changes from the prior version are listed in the Change History.

Change History

Date	Changes
4/12/2016	v1.1 – Update • Changed name from "Standards" to "Policy" • Removed document numbering • Tailored content for general users' use • Differentiated between access requests for enterprise systems and access that is administered by business owners • Clarified acceptable uses of RTD technology and consequences for inappropriate use • Added physical security and asset management requirements for technology requirements

	• Added clarification to regarding personal device use, scanning, and possible document discovery activities • Enhanced system lock and logout requirements • Added policies for network access • Updated password policy to include more stringent requirements • Added security requirements for screen sharing and remote control sessions • Enhanced, clarified, and simplified security requirements for sensitive information • Clarified management responsibility to establish personal use restrictions and monitor for compliance • Clarified security incident reporting requirements • Added training requirements • Established violations and exceptions policies • Enhanced security requirements for mobile devices • Removed cell phone provisions (refer to Cell Phones Management Directive) • Removed CORA/document retention references (refer to Records Management Policy) • Added an annual review cycle for the policy • Updated Document Contacts to reflect changes in leadership • *Note: Separate policies were created for IT administrators: IT Security Policy for Enterprise Systems*
5/5/2014	v1.0 - Initial Release

Document Contacts

Contact	Sheri Le, Manager of Cybersecurity
Author	Sheri Le, Manager of Cybersecurity
Content Coordinator	Sheri Le, Manager of Cybersecurity
Business Owner	Kim Heldman, Senior Manager of IT
Executive Owner	Heather Copp, AGM, Finance & Administration

Secure Computing Standards

Confirmation of Receipt and Understanding

I certify that I have received a copy of, read, and understood the requirements of the RTD Secure Computing Policy. I understand that I am responsible to comply with the requirements of this policy in all circumstances in which I am using RTD technology equipment or services as defined by the policy. I further understand that my use of RTD technology equipment or services may be monitored by management at any time, for any reason, and revoked without prior notice if I am found to be in violation of this policy in order to preserve the availability and integrity of RTD technology resources for other computer users and to protect the security of RTD business operations.

Further, I acknowledge that if I choose to use a personal device to access RTD information (e.g. RTD email) and that device is ever lost or stolen, I am required to promptly notify RTD IT of that incident. I understand that RTD, at its sole discretion, may remotely wipe the device, resulting in the loss of all local data on that device.

Please list any personal devices that you currently use or anticipate using for work at RTD (e.g. personal smartphone, iPad, etc.):

_____

_____

_____

Printed Name: _____

Signature: _____

Date: _____

If you are reviewing an online copy of this policy, please indicate your review and understanding of the policy and, if applicable, your current list of personal devices on the certification website. A paper form is not necessary.

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

B. RTD-CYBER-VR-05: Commercial Product Purchases Vendor Requirements

COMMERCIAL PRODUCT PURCHASES VENDOR REQUIREMENTS

RTD-CYBER-VR-05
Version 4

Commercial Product Purchases

"**Product**" means any commercial off-the-shelf computer hardware or software component provided by a Contractor (e.g. reseller) that will become property of RTD via physical acquisition or be licensed for use by RTD and will be used on the RTD network or in conjunction with other RTD technologies.
"**Networked product**" means any hardware or software component that must communicate or integrate with another device on the RTD network or across the Internet.
"**Safety or security sensitive**" means that while in use at RTD, the product will play a critical role in passenger or employee safety or security functions. In the Industrial Control Systems (ICS) context, products that are used in safety zones (safety domains) or have the ability to influence the safety zone are considered safety or security sensitive.

1. **Minimum Viable Use.** The product shall have a minimum viable use of three years from the date of purchase. Products that are end of life or scheduled for sunset within three years of the date of purchase are ineligible. Should the product purchase be part of an overarching service contract that includes the ongoing purchase, installation, and maintenance of commercially-available equipment over a fixed term, purchased products must be replaced when they reach end-of-life status.
2. **Patches and Upgrades.** Should the product include software or firmware components, to maintain the currency, supportability, and security of the product software or firmware, the product shall be accompanied by a maintenance or licensing agreement that shall, at minimum, include patches for security and bug fixes (including roll up packages for updates, e.g. service packs) and incremental version upgrades for no less than three consecutive years from the installation date. Should the Contractor not be performing the regular installation of these patches or updates under the Agreement at initial installation or after the initial installation, the Contractor shall provide clear and unambiguous written instructions to RTD on how to acquire and install the patches or updates, including but not specifically limited to any relevant and necessary bulletins, websites, manuals, or service contacts.
3. **Implementation Guide.** The product shall be accompanied by clear and unambiguous written instructions (e.g. a manual or product implementation guide) on how to set security features for the product. At minimum, the instructions shall address access control features, including changing of default user IDs and passwords post-installation and managing encryption keys (as applicable). For networked products, the instructions shall additionally include a list of the minimum necessary services, ports and protocols required to facilitate communication between this product and others (e.g. a database server).
4. **Responsible Sourcing.** Products with Department of Homeland Security directives against purchase or that are sold or manufactured by companies on the Department of Labor Office of Federal Contract Compliance Programs Debarred Companies list are ineligible. Additionally, to the extent that it is possible to provide, the Contractor shall provide RTD with additional information about the manufacture or acquisition of safety or security sensitive products to ensure they are responsibly sourced and reduce the risk of embedded threats and vulnerabilities.

5. **Logging.** The product must support or facilitate logging and forwarding of application security events for operational failure, security incident, and security monitoring purposes.
6. **Access Control and Authority.** The product must contain features that allow administrators to control user and system access to functions, features, or system components a need-to-know basis. The product must be able to operate with user level authority, and must not require that a user be logged in as an administrator in order to operate properly. Users and administrators of the product must be able to change and otherwise manage their credentials (for example, establish a password and perform password resets).
7. **Compatibility with Security Functions and Products.** The product must be capable of operating concurrently with well-known industry security products, such as antimalware programs, log collection and monitoring agents, and web application firewalls. The product must tolerate periodic vulnerability scanning, operating system patching and upgrades, and basic system hardening (for example, changing of default passwords and disabling unnecessary services). Products that require an out-of-support operating system or do not tolerate operating system patching for at least three years from the date of purchase will be considered out of compliance with the Minimum Viable Use requirement.
8. **Data Security.** Products that are intended for the storage, processing, or transfer of sensitive data must support strong encryption at rest. Products that communicate over the Internet, for example, for authentication, maintenance purposes, or remote management, must use unbroken encrypted communication methods. Products that store sensitive data must tolerate and/or enforce purging data that RTD determines no longer has a business need to be retained.
9. **Proof of Concept.** Proof of concept systems and environments must be physically and logically separate from RTD production systems and must not require the use of any production RTD data.
10. **Exceptions.** Should a product be necessary to fulfill the scope of services under the Agreement, yet incapable of conforming to some or all of the aforementioned requirements, the Contractor shall identify the non-conforming product to RTD and the specific requirements that are not met to afford RTD the opportunity to understand the risks to RTD's operations. The Contractor shall additionally explore and present alternatives, including but not limited to use of a different product, configuration options, or other risk mitigation measures, and present those opportunities to mitigate risk (if any) to RTD. The Contractor shall not install a non-conforming product without RTD's written approval.

ADDITIONAL RESOURCES

- [Text or bulleted links.]

REVISION HISTORY

10/28/2019 – Initial Draft – [SAR]
10/28/2020 – Added Revision Section – [MB]

01/05/2021 – Removed tables and added version and date to name of document – [MB]
01/06/2021 – Updated document with RTD business template – [MB]

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

C. RTD-CYBER-VR-10: Network Access Vendor Requirements

NETWORK ACCESS VENDOR REQUIREMENTS

RTD-CYBER-VR-10
Version 4

Network Access

"RTD Network" refers to any computer networks that are hosted, maintained, and operated by RTD.

"RTD Facilities" refers to any RTD maintained and operated location that is physically accessible; for example: offices, data centers, stations, communications closets or houses, maintenance facilities, sheds or outbuildings, utility conduits, and handholds.

1. **RTD Security Policies and Procedures.** In the event the Contractor's personnel or subcontractors require access RTD facilities, network, or related systems, whether physically or remotely, in order to provide installation, integration, interconnection, support, or other services, Contractor will abide by RTD's internal security policies and procedures.
2. **Contractor Access Requests.** Should Contractor access to RTD facilities or networks be necessary to support the implementation or support of the Services, Contractor shall document the contact information for the individuals requiring access, the necessary level of access, and the business justification for each access in their request for access to RTD. Contractor will not share access among multiple individuals working for the same Contractor or with subcontractors.
3. **Access Limitations**. Contractors will be provided with the least amount of access to facilities, systems, networks, and data necessary to perform the Services. RTD shall determine the degree and methods of access necessary to support the scope of services per applicable internal security policies and procedures.
4. **Access Termination**. Contractor must notify the RTD Sponsoring Manager immediately upon actual or anticipated departure or change in job role for Contractor personnel with access to the RTD network.
5. **Personnel Security.** Contractor must furnish evidence of a successful background check, and if applicable, signed non-disclosure agreements prior to requesting access to the RTD Network or Facilities.
6. **Security Control Non-Disclosure.** The Contractor shall not publish or disclose in any manner the details of any safeguards designed to protect RTD facilities or networks without prior consent of RTD.

Summary of RTD's Internal Security Policies

- **Acceptable Use of Technology**: RTD technology equipment is for RTD business use only.
- **Computer System and Network Configuration:** All installed equipment shall conform to RTD's policies, procedures, and standards for system configuration.
- **Electronic Data Protection:** Electronic sensitive and confidential information shall be access controlled.
- **Computer System Activity Logging and Monitoring:** All business-critical systems shall be logged and monitored for operational and security failures.

- **Computer System and Electronic Data Access Control:** Access to RTD systems and data is provisioned based on documented approval, business justification, and in keeping with the principle of least privilege.
- **Information Technology Risk Management:** Risks shall be assessed before new technology systems are launched; appropriate RTD management shall make informed decisions regarding risk treatment.
- **Cybersecurity Incident Response:** Incidents shall be reported, categorized / prioritized, and responded to in a consistent manner.
- **Secure Application Acquisition and Development:** Developed or purchased applications shall conform to RTD's policies, procedures, and standards for applications.
- **Vendor Cybersecurity Management**: Contractors for vendor services and products shall include RTD's cybersecurity requirements; performance to such shall be monitored by the contract sponsor.

ADDITIONAL RESOURCES

- [Text or bulleted links.]

REVISION HISTORY

10/28/2019 – Initial Draft – [SAR]
10/28/2020 – Added Revision Section – [MB]
01/05/2021 – Removed tables and added version and date to name of document – [MB]
01/06/2021 – Updated document with RTD business template – [MB]

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

D. RTD-IT-PLY-0001: Acceptable Use of RTD Technology Policy

Policy Name:	Acceptable Use of RTD Technology				
Policy #:	RTD-IT-PLY-0001	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration - Information Technology				

1. POLICY STATEMENT

Employees and contractors shall use RTD computers and communication systems primarily for the purpose of conducting RTD business and in a manner consistent with the District's standards for business conduct.

All technology users shall comply with RTD policies and procedures regarding the maintenance, inventory, and disposal of the equipment assigned to them and the information that it contains, and shall physically safeguard all technology devices in their care against theft and misuse.

RTD may monitor employee and contractor use of RTD technology resources at any time to detect signs of a cybersecurity compromise or violations of RTD policy. Employees and contractors should have no expectation of privacy when using RTD's technology resources.

2. PURPOSE

This policy provides guidance regarding business use of RTD computers and communication systems to promote the safe, efficient, and responsible use of RTD technology resources, and protect the integrity, stability, security, and supportability of technology-enabled business services.

3. SCOPE

This policy applies:

- To all computers, computerized equipment, and computer-enabled functions (including laptops, desktops, tablets, smartphones, wireless or wired networks/Internet connection, servers, control systems, phones, portable storage media, and specialized systems and appliances) owned and managed by RTD and their respective operating systems, file systems, and applications

- To both physical and logical computer system components
- To all externally-hosted or contracted computing services (including servers, networks, custom and commercial applications, and cloud-based services) that are used to perform RTD business functions
- To all electronically stored information (data) owned and maintained by RTD in the aforementioned systems, repositories, or applications
- To all internal business networks owned and operated by RTD, both wireless and hard-wired
- To all employee or contracted staff that use RTD computer systems

4. RESPONSIBILITIES

RTD employees and contractors – use RTD technology and secure and dispose of assigned technology assets (ex. computer systems) only in accordance with this policy and related procedures.

Managers/supervisors – monitor for and enforce appropriate uses of technology among their staff. Manage the use, security, and disposal of any technology assets that are owned by or assigned to their departments.

Information Technology department (or alternative equipment managers) – manage technology and procedures that support appropriate use, security, and disposal of assets in accordance with established RTD policy, procedure, and management direction. Notify managers and supervisors, and if necessary, engage the Cybersecurity Incident Response Procedure to address instances of suspected policy violations, abuse, or compromise.

Safety, Security, and Asset Management – provide agency-wide physical security, acquisition, and disposal policies and procedures to facilitate the protection and management of RTD physical assets.

5. SUPPLEMENTAL GUIDELINES

Employees and contractors may use RTD's technology equipment and internal business network for brief, incidental personal purposes provided that the use is consistent with the existing technology or network configuration, of nominal operational and security risk and impact, and is inconsequential to the performance of the employee or contractor's duties.

- Examples of **permitted** personal use include, but are not limited to, checking travel plans, email, weather, or reading articles on the web.
- Examples of **prohibited** personal use include constant personal streaming of movies or music, gaming, and downloading, uploading, or storing significant volumes of personal content on an RTD workstation or server.

RTD Information Technology may block protocols, services, or sites that are primarily for personal use and interfere with the stability or efficient operation of the RTD business network.

Employees and contractors should refrain from connecting personal or non-RTD company devices (phones, laptops, tablets) to RTD's internal business network. Employees, contractors, vendors, and guests who would like to use a personal or non-RTD company device at RTD, for example, while on break or to conduct a demonstration, may use RTD's guest wireless networks. Employees and contractors who have a business need to use a personal or non-RTD company device on RTD's business network must abide by RTD's Bring Your Own Device (BYOD) policy.

6. RESOURCES

RTD Code of Ethics

RTD Employee Guidelines (Salaried and Represented)

Social Media Guidelines

Bring Your Own Device (BYOD) (forthcoming)

PCI-DSS v. 3.2, Requirement 9, 12

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-10
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance:			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

E. RTD-IT-PLY-0002: Computer System and Network Configuration Policy

Policy Name:	Computer System and Network Configuration				
Policy #:	RTD-IT-PLY-0002	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration - Information Technology				

1. POLICY STATEMENT

All RTD computer users and system administrators shall configure RTD-owned networks and computer systems in a manner that conforms to RTD's current software, maintenance, and technical configuration procedures, standards, and relevant system security plan(s). Computer users may not change, uninstall, or turn off any of the required security software or standard configuration parameters on RTD-managed systems at any time, for any reason.

RTD system administrators shall configure new systems and networks in a manner that conforms to the most recent procedures, standards, and security plans at the time of installation. RTD system administrators shall thereafter periodically evaluate system and network compliance to the most recent procedures, standards, and security plans prior to any major configuration changes; when relevant configuration procedures, standards, and security plans change; and otherwise periodically.

2. PURPOSE

This policy prevents computer users and system administrators from configuring RTD-owned networks and computer systems in a less-than-secure manner. Secure configuration promotes the stability, supportability, and safety of RTD's technology-enabled business services.

3. SCOPE

This policy applies:

- To all computers and computerized equipment (including workstations, networks, servers, control systems, and specialized systems and appliances) used at RTD and their respective operating systems, file systems, and applications

- To all externally-hosted or contracted computing services (including but not limited to servers, networks, custom and commercial applications, and cloud-based services) that are used to perform RTD business functions or manage RTD data
- To all employees or contracted staff that use, manage, install, and/or configure RTD computer systems or electronic data

4. RESPONSIBILITIES

RTD employees and contractors (computer users) – use computer systems in a manner that maintains conformance to the configuration requirements.

System administrators – configure RTD-managed systems in accordance with RTD standards and security plans prior to initial deployment. Evaluate compliance to plans and standards prior to major changes, when configuration standards and security plans changes, and otherwise periodically.

Business process owners – participate in testing and designing secure configurations for the system(s) that support their business process, as applicable

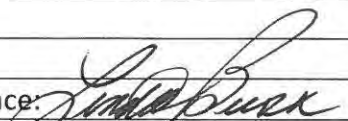
Information Technology department – in conjunction with the system administrator, identify software, maintenance, and technical configuration standards and security plans for each system type.

5. RESOURCES

PCI-DSS v. 3.2, Requirements 1, 2, 6, 8, 11, 12

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-10
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance: 			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

F. RTD-IT-PLY-0003: Electronic Data Protection Policy

Policy Name:	Electronic Data Protection				
Policy #:	RTD-IT-PLY-0003	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration – Information Technology				

1. POLICY STATEMENT

RTD employees and contractors shall use available technical security measures to protect electronic RTD data from inappropriate disclosure, loss, or corruption, in accordance with its business use and sensitivity classification.

RTD employees and contractors shall always encrypt confidential and sensitive data when it is transmitted externally (ex. across the Internet). Where possible, RTD employees and contractors shall encrypt internal RTD confidential and sensitive data while in transit between or at rest on RTD systems. RTD employees and contractors shall only use encryption methods that are approved and supported by the Information Technology department (or other data custodian, as applicable).

If encryption is not possible or an approved method is not yet available, RTD employees and contractors shall use standard procedural and technical security measures to protect internal sensitive and confidential data from disclosure in transit and at rest (for example, access controls, password protection).

2. PURPOSE

This policy prevents electronic RTD information from being inadvertently disclosed to, corrupted by, or lost because of the actions of unauthorized persons or processes. This policy additionally prevents users from damaging or destroying RTD information because they do not have the expertise or knowledge required to use encryption methodologies properly.

3. SCOPE

This policy applies:

- To all computers and computerized equipment (including workstations, networks, servers, control systems, and specialized systems and appliances) owned and managed by RTD and their respective operating systems, file systems, and applications
- To all externally-hosted or contracted computing services (including but not limited to servers, networks, custom and commercial applications, and cloud-based services) that are used to perform RTD business functions or manage RTD data
- To all electronically stored information (data) owned and maintained by RTD in the aforementioned systems, repositories, or applications
- To all RTD employees or contracted staff that manage access to electronic data independently or as assisted by a data custodian, service, or application

4. RESPONSIBILITIES

RTD employees and contractors (data users) – use available, appropriate, and approved data security technologies to protect RTD electronic data from inappropriate disclosure, loss, or corruption. Manage any independently generated passwords or keys required to facilitate secure access to the data. Report any inappropriately-controlled or uncontrolled data encountered to the data owner for remediation.

Business process owners (data owners) – identify the types, locations, lifecycle, and classification of electronic data that they own and manage.

Information Technology department (or alternative data custodian) – identify, approve, make available, and manage data security technologies, including encryption technologies. Manage any centrally-generated passwords or keys required to ensure availability to the data. Recover lost or corrupted data where feasible.

5. RESOURCES

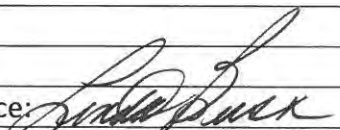
RTD-GC-PLY-0001 Confidential and Sensitive Information Policy

RTD-IT-PLY-0005 Computer System and Electronic Data Access Control Policy

PCI-DSS v. 3.2, Requirements 3, 4, 9, 12

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-03
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance: 			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

G. RTD-IT-PLY-0004: Computer System Activity Logging and Monitoring Policy

Policy Name:	Computer System Activity Logging and Monitoring				
Policy #:	RTD-IT-PLY-0004	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration - Information Technology				

1. POLICY STATEMENT

RTD system administrators shall configure business-critical application systems, infrastructure systems, and security management systems to generate, and centrally maintain logs of system-level activity in a manner consistent with the applicable system security plan(s) for the monitored system and/or business operational and security best practices.

RTD system administrators, or an equivalent monitoring facility, shall monitor logs for operational failures and suspicious activity. RTD system administrators shall strictly control access to logs to maintain log integrity and availability. The Information Technology (IT) department (or responsible log custodian, if not IT) shall maintain adequate storage, staff, and technical capability to support log retention and monitoring.

2. PURPOSE

This policy ensures that all RTD business-critical computer systems have an audit log that can be examined to monitor for and assist with the investigation and resolution of operational problems and security incidents. This policy additionally ensures that enough logs are retained, and retained securely, to provide accurate, detailed evidence of the timeline and sources of a security breach, should one occur.

3. SCOPE

This policy applies:

- To all RTD-owned and managed multi-user computers and computerized equipment that is operationally critical and/or performs a security function, including network equipment, servers, control systems, and specialized systems and appliances used and their respective operating systems, applications, and databases.

- To all externally-hosted multi-user computers and computerized equipment that is used to perform operationally critical and/or security functions on behalf of RTD, including network equipment, servers, control systems, and specialized systems and appliances and their respective operating systems, applications, and databases.
- To any other computer system as required by the respective system security plan(s) or regulations that pertain to that system type.
- To all RTD system administrators or contractors who perform system administration services on behalf of RTD.

4. RESPONSIBILITIES

Business process owners – provide context for the system events that are recorded and monitored to Information Technology such that they may screen normal from anomalous activity and take appropriate action.

System administrator – configure systems that they administer to generate and store logs; monitor the systems for operational failures and suspicious activity; enact appropriate analysis and response procedures when an anomalous event is detected.

Information Technology department (or similar log custodian) – identify, maintain, and secure the log storage and monitoring systems and the log data that they contain or access.

5. RESOURCES

PCI-DSS v. 3.2, Requirement 10

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-03
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance:			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

H. RTD-IT-PLY-0005: Computer System and Electronic Data Access Control Policy

Policy Name:	Computer System and Electronic Data Access Control				
Policy #:	RTD-IT-PLY-0005	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration - Information Technology				

1. POLICY STATEMENT

RTD system administrators shall only grant access to RTD computer systems or electronic RTD data to individuals with a documented and manager-approved business justification for access. System administrators shall assign each access identifier to a unique owner (i.e. a person). System administrators shall grant only the minimum amount of access required to accomplish the stated business purpose and deny all other access by default.

2. PURPOSE

This policy ensures that computer users acquire and retain only the least necessary level of access to RTD systems and information that they need to perform their job duties to prevent inappropriate disclosure or changes to RTD information and reduce the chances of intentional or unintentional harm to or interruption of RTD's business services. The policy additionally ensures clear lines of accountability for all access granted to RTD systems and information for access verification and inspection purposes.

3. SCOPE

This policy applies:

- To all computers and computerized equipment (including workstations, networks, servers, control systems, and specialized systems and appliances) owned and managed by RTD and their respective operating systems, file systems, and applications
- To both physical and logical computer system components
- To all externally-hosted or contracted computing services (including but not limited to servers, networks, custom and commercial applications, and cloud-based services) that are used to perform RTD business functions or manage RTD data

- To all electronically stored information (data) owned and maintained by RTD in the aforementioned systems, repositories, or applications
- To all employee or contracted staff that have or require access to RTD computer systems or electronic data

4. RESPONSIBILITIES

RTD employees and contractors – provide a documented business justification for access.

Managers/supervisors – review and approve employee and contractor requests for access; notify Information Technology and/or the access manager to revoke access when the business need for access no longer exists.

Business process owners – review and approve manager-validated access requests to verify applicability and appropriateness to the systems or data repositories that they manage.

Information Technology department (or alternative system administrator) – identify and manage the specific procedures to intake access requests, validate approval for access, provision access, revoke access, and maintain computerized access control systems.

5. RESOURCES

PCI-DSS v. 3.2, Requirement 7

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-05
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance:			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

I. RTD-IT-PLY-0006: Information Technology Risk Management Policy

Policy Name:	Information Technology Risk Management				
Policy #:	RTD-IT-PLY-0006	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration – Information Technology				

1. POLICY STATEMENT

System administrators and owners of business-critical information systems shall assess risk to critical RTD business operations or the security of RTD staff or passengers prior to putting new information technology products and services in operation, with every major change to existing technology products and services, as determined necessary by management to gauge RTD's level of risk preparedness, and otherwise periodically.

Risk assessors engaged to perform such reviews shall document and maintain procedures and consistent methodologies for conducting the risk reviews and shall review all significant risks discovered with the system administrator, business owner of the system, the responsible Assistant General Manager, and the Risk Management Department following the assessment. The responsible Assistant General Manager and business owner of the system shall determine whether and when the risks will be corrected, mitigated, or formally accepted by RTD. The responsible Assistant General Manager and business owner of the system shall, with the assistance of the risk assessor, periodically review residual (accepted) risks in light of then-existing RTD capabilities and the present threat climate to determine whether continued acceptance or action is appropriate.

2. PUROPSE

The policy ensures that critical technology risks are consistently identified and raised to management, and identifies who among RTD management is accountable to make conscious, informed decisions regarding whether and how to address risks to limit the likelihood of adverse impact to RTD's safety and operational stability.

3. SCOPE

This policy applies to enterprise and end user computer systems; cloud and technology products and services; and data centers that are managed by Information Technology (IT) staff internally or on behalf of the RTD organization. This policy also applies to computer

systems and data centers that are managed by Operations teams (ex. control systems, SCADA), or independent departments.

4. RESPONSIBILITIES

Assistant General Managers – decide if and how enterprise-level risks shall be addressed as they are reported by IT, business process owners, managers, and supervisors.

Risk Management Department – assess, track, report, and mitigate risks in the context of RTD's overall business services.

Information Technology (IT) Department (or alternative department by role)

- **Risk assessor** - maintain procedures and assign staff to assess and track technology-related risks; report significant technology risk to RTD upper management and the RTD Risk Management Department. For small-scale efforts, the risk assessor may be the system administrator or business owner.
- **System administrator** - initiate risk review; participate in the risk assessment process; evaluate risks that are reported by the risk assessor, managers, or supervisors for impacts to system operations; recommend and implement solutions to mitigate risk as necessary.

Business Owner – initiate risk review; participate in the risk assessment process; evaluate risks that are reported by the risk assessor, managers, or supervisors for impacts to business processes; decide whether and how the risk should be managed; recommend and implement solutions to mitigate risk, as necessary.

Employees and Contractors – understand, assess, and report risks associated with technologies used in their job roles to their manager or supervisor and IT.

5. RESOURCES

PCI-DSS v. 3.2 Requirements 11, 12

NIST Special Publication 800-39: Managing Information Security Risk (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-10
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance:			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

J. RTD-IT-PLY-0008: Cybersecurity Incident Response Policy

Policy Name:	Cybersecurity Incident Response				
Policy #:	RTD-IT-PLY-0008	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration – Information Technology				

1. POLICY STATEMENT

RTD employees and contractors shall immediately report known or suspected cybersecurity incidents to their management and the IT Service Desk. RTD employees and contractors shall participate in cybersecurity awareness training at least annually to help them identify and avoid cyber-incidents.

Departments that manage RTD technology, including but not limited to the RTD Information Technology Department, shall organize and maintain an in-house Cybersecurity Incident Response Team (CIRT) that shall provide accelerated problem notification, damage control, and problem correction services in the event of computer related incidents. CIRT response procedures shall include, at minimum, the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. CIRT members shall test their response procedures at least annually.

2. PURPOSE

This policy ensures that cybersecurity incidents are reported and investigated in a timely, consistent manner to minimize disruption of services, inappropriate use of RTD's resources, and corruption or unauthorized disclosure of sensitive information belonging to the agency, RTD's employees, partners, or customers.

3. SCOPE

This policy applies:

- To all events involving or in which it is suspected that a security compromise may have occurred or is occurring
- To all business-critical systems requiring immediate response in the event of an outage

- To all events involving a widespread outage of the aforementioned business critical resources
- During regular and non-regular business hours (24x7) including weekends and holidays
- When a full incident response is otherwise required by management, outside of the circumstances above, to provide an immediate coordinated response

4. RESPONSIBILITIES

RTD employees and contractors – report any known or suspected cybersecurity incidents immediately to the IT Service Desk; participate in cybersecurity awareness training.

Information Technology Department (or other departments that manage technology, as appropriate) – Identify CIRT members, document incident response procedures, train staff in incident response procedures, and test procedures annually.

Cybersecurity Incident Response Team (CIRT) – follows the documented response procedure to analyze, classify, contain, and eradicate the incident.

Business process owners – contribute to incident response at the direction of the CIRT, authorize changes to systems that support business processes, and enact business continuity and regulatory or legal reporting procedures as necessary.

5. RESOURCES

PCI-DSS v. 3.2, Requirement 12.10

NIST Cybersecurity Framework (https://www.nist.gov/cyberframework)

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-05
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance:			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

K. RTD-IT-PLY-0009: Secure Application Acquisition and Development Policy

Policy Name:	Secure Application Acquisition and Development				
Policy #:	RTD-IT-PLY-0009	Date Issued:	2018-07-13	Current Version	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:					

1. POLICY STATEMENT

RTD employees and contractors shall only purchase and deploy applications that both independently conform to, and allow users of the application to comply with, RTD's computer security policies, procedures, and standards.

All RTD or contracted application developers shall additionally adhere to the secure coding best practices relevant to their coding language or framework when creating or customizing RTD business applications. All RTD application developers shall train in secure coding principles at least annually. At least one employee on each development team shall maintain an industry-recognized certification in secure application development principles.

2. PURPOSE

This policy ensures that applications that are purchased or created by RTD and used for RTD business purposes are designed and deployed with security in mind, so as to promote the stability of RTD's technology-enabled business services and the security of the data processed and business functions handled by the application.

3. SCOPE

This policy applies to:

- All RTD information system applications that are acquired (pre-built, commercial-off-the-shelf, or Software-as-a-Service/cloud applications), developed in-house, or developed using outside parties
- All RTD application developers, including but not specifically limited to those that are members of the Information Technology or Marketing departments

4. RESPONSIBILITIES

RTD employees and contractors – select and deploy only those applications that are designed to or otherwise capable of meeting RTD's computer security policies, procedures, and standards either by participating in secure development processes (requirements gathering) and/or by including and enforcing contract requirements for externally-supported projects.

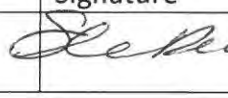
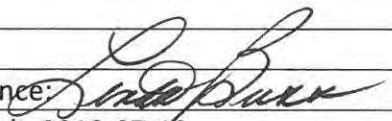
Application developers – use secure development practices in the coding, integration or customization, testing, and documentation of custom RTD business applications; train at least annually in secure coding practices; as applicable, maintain secure coding certification(s).

Managers/supervisors – ensure that their staff understands their responsibilities under this policy; identify and correct any gaps in compliance to this policy; enable application development staff to train and maintain certifications in secure coding.

5. RESOURCES

PCI-DSS v. 3.2 Requirement 6: Secure application development

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-05
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance: 			
Version: A		Date issued: 2018-07-13	

SUPPLEMENTAL TECHNOLOGY TERMS AND CONDITIONS

ADDITIONAL RTD POLICIES

L. RTD-IT-PLY-0019: Vendor Cybersecurity Management Policy

Policy Name:	Vendor Cybersecurity Management				
Policy #:	RTD-IT-PLY-0019	Date Issued:	2018-07-13	Current Version:	A
General Manager Approval:					
Assistant General Manager Approval:					
Responsible Department:	Finance and Administration – Information Technology				

1. POLICY STATEMENT

All RTD employees involved specifying or selecting commercial products or services that include technology components or entail the development, customization, or integration of custom technology products shall clearly specify requirements for and/or evaluate conformance to RTD's established cybersecurity policies, procedures, and standards, in all contracts, license agreements, or other external-party agreements prior to purchase.

Business owners of purchased products and services shall monitor vendors' continued adherence to RTD's security requirements throughout the life of the product or contract. Business owners shall raise any noted departures from RTD's security requirements both prior to and at any time after the time of purchase to their purchasing agent, General Counsel, and/or their management's attention for evaluation in accordance with the Information Technology Risk Management policy and contract performance management best practices.

2. PURPOSE

This policy ensures that technology products purchased by RTD are capable of meeting RTD's security policies, procedures, and standards, and that RTD can hold vendors accountable to meet our security requirements when performing technology services, thus reducing the risk to RTD of unclear or unsecure products and service providers being introduced to or operating critical RTD business services.

3. SCOPE

This policy applies to:

- All RTD information system applications that are acquired (pre-built, commercial-off-the-shelf, or Software-as-a-Service/cloud applications), developed in-house, or developed using outside parties

- All RTD application developers, including but not specifically limited to those that are members of the Information Technology or Marketing departments

4. RESPONSIBILITIES

RTD employees and contractors – identify security requirements that are relevant to the product or service that they are requesting or evaluating; evaluate a vendor's or product's ability to conform to RTD's requirements and investigate residual risks.

Business owners – select vendor products and services that meet RTD's security requirements; continually evaluate and manage the vendor's or product's conformance to RTD's most recent security requirements; address and/or clarify any gaps in requirements or performance with vendors; raise any noted risks (gaps) to the purchasing agent, general counsel, and management for evaluation.

Information Technology department (risk assessors) – counsel business owners of vendor products and services and other RTD employees and contractors on the most appropriate requirements to include given the product or service business use case; assist business owners and RTD employees and contractors to understand and qualify gaps in requirements in preparation for risk assessment.

Managers/supervisors – review and qualify any gaps in the vendor's capability or performance relative to RTD's security requirements and the product or service business use case; determine how to address gaps in accordance with the Information Technology Risk Management policy.

Purchasing agents – verify that security requirements are attached to, included, or reviewed for every purchase involving technology products or services prior to requesting proposals or proceeding with a purchase; assist with addressing contract changes at the direction of the business owner, manager/supervisor, and general counsel.

General Counsel – assist with addressing contract performance issues in conjunction with the business owner, manage/supervisor, and general counsel.

5. RESOURCES

PCI-DSS v. 3.2 Requirement 12: Vendor management

REVISION BLOCK

Draft prepared by:			
Name	Signature	Position	Date
Sheri Ricardo		Manager of Cybersecurity	2018-07-05
Description of Revision(s): New policy.			
Reviewed by:			
Information Governance and Management Division Acceptance:			
Version: A		Date issued: 2018-07-13	

EXHIBIT 1

CONTRACTOR'S KEY PERSONNEL

The personnel listed below are considered to be essential to the Work required under this Contract. Prior to removing any key personnel from Contract Work, the Contractor shall notify RTD within 14 days of such proposed removal and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the Contract. No removal of key personnel shall be made by the Contractor without the written consent of RTD by Contract Amendment.

Name	Title	Company

EXHIBIT 2
REGIONAL TRANSPORTATION DISTRICT
INSURANCE & BOND REQUIREMENTS
PROFESSIONAL SERVICES CONTRACTS

General

All defined terms contained in this Exhibit 2 shall have the same meaning ascribed to them in the **Contract**.

The **Contractor** shall procure and maintain, and shall require that its subcontractors purchase and continuously maintain in full force and effect for the **Contract** period specified herein, all insurance policies specified in this Exhibit 2. The **Contractor** shall forward updated certificates of insurance and endorsement(s) when policies are renewed or changed.
The insurance required hereunder shall not be interpreted to relieve the **Contractor** of any obligations under the **Contract**, and liability of **Contractor** under this Exhibit 2 shall not be limited to coverage provided under said insurance policies. The **Contractor** and its subcontractors shall remain solely and fully liable for all deductibles, self-insured retentions, and amounts in excess of the coverage actually realized.

Commercial General Liability Insurance

At all times during the performance of the **Contract**, the **Contractor** and its subcontractors shall have and maintain Commercial General Liability Insurance insuring against claims for bodily injury, property damage, personal injury and advertising injury. By its terms or appropriate endorsements such insurance shall include the following coverage: Bodily Injury, Property Damage, Fire Legal Liability, Personal Injury, Blanket Contractual, Independent Contractors, Premises Operations, Products and Completed Operations Hazard for a minimum of two (2) years following final completion of the Project or the applicable statute of limitations or statute of repose, whichever is greater. The policy cannot be endorsed to exclude cause of loss related to earth movement, explosion, collapse and underground exposures without the specific written approval of RTD, nor may the policy exclude or limit **Contractor's** or its subcontractors' liability for acts or omissions of any independent contractors or subcontractors, nor may the policy exclude work of any independent contractor or subcontractor; nor contain any conditions regarding when coverage is available for acts, omissions or work of a **Contractor** or subcontractor, nor may the policy limit coverage to a designated premises, nor may the policy exclude or limit coverage for liability arising from the Products and Completed Operations Hazard.

If any Work performed under this **Contract** is within fifty (50) feet of RTD's light rail or commuter rail alignment, then the **Contractor** and its subcontractors shall have and maintain ISO form CG 2417 1001 - Contractual Liability – Railroads.

If Commercial General Liability Insurance or other form with general aggregate limit and products and completed operations aggregate limit is used, then the aggregate limits shall apply separately to the Project, or the **Contractor** and/or its subcontractors may obtain separate insurance to

provide the required limit which shall not be subject to depletion because of claims arising out of any other project or activity of the **Contractor** and/or its subcontractors. General Aggregate limit applies per construction Project.

The policy or policies must provide the following minimum limits of liability as follows:

Amount of Coverage:	$1,000,000 per occurrence $2,000,000 aggregate

There shall be a separate minimum limit of liability for the Products/Competed Operations Hazard not included within the General Aggregate.

Amount of Coverage	$1,000,000 per occurrence $2,000,000 aggregate

Commercial Automobile Liability Insurance

At all times during the performance of the **Contract**, the **Contractor** and its subcontractors shall have and maintain Automobile Liability Insurance insuring against claims for bodily injury and property damage arising out of the ownership, maintenance or use of all owned/leased as well as hired and non-owned vehicles. The Automobile Liability policies shall have minimum limits of liability as follows:

Amount of Coverage:	$1,000,000 combined single limit

Workers' Compensation and Employer's Liability Insurance

At all times during performance of the **Contract**, the **Contractor** and its subcontractors shall each have and maintain Workers' Compensation Insurance sufficient to meet its statutory obligations to provide benefits for their contractual and statutory employees with claims of bodily injury or occupational disease (including resulting death).

The **Contractor** and its subcontractors shall each provide Employer's Liability Insurance covering their legal obligation to pay damages because of bodily injury or occupational disease (including resulting death) sustained by their contractual and statutory employees with minimum limits of liability as follows:

Amount of Coverage:	$1,000,000 bodily injury by accident $1,000,000 bodily injury by disease $1,000,000 policy limit

Umbrella/Excess Liability

At all times during performance of the **Contract**, the **Contractor** and its subcontractors shall have and maintain Umbrella and Excess Liability insurance on a following form basis with limits of liability in a minimum amount as follows for a minimum of two (2) years following final completion of the Project or the applicable statute of limitations or statute of repose, with minimum liability limits as follows:

Amount of Coverage:	$5,000,000 per occurrence $5,000,000 aggregate

This excess insurance shall follow form and be at least as broad as the **Contractor's** and/or its subcontractors primary Commercial General Liability (including additional insureds), Commercial Auto Liability, and Employer's Liability insurance. The above insurance levels may be met through any combination of primary insurance and excess liability/umbrella insurance so long as the total amount meets the stated minimum requirements.

Professional Liability

When a **Contractor**, subcontractor, vendor or supplier has a professional designation or license and/or is providing professional services, at all times during the performance of this **Contract**, the **Contractor** and/ or subcontractors shall have and maintain a Professional Liability (Error and Omissions) policy. This insurance shall be maintained for the duration of the **Contract** and for a minimum of two (2) years following completion of the **Contract** or the applicable statute of limitation or statute of repose, whichever is greater. The minimum limit for architects and engineers is $5,000,000 per claim and in the aggregate and may be increased depending upon the nature of the services to be provided to RTD. The minimum limits of liability for other **Contractors** and/or subcontractors is:

Amount of Coverage:	$2,000,000 per claim $2,000,000 aggregate

Cyber Risk Insurance

When a **Contractor**, subcontractor, vendor, supplier or any third-party will be using, storing or accessing private, confidential or protected information on behalf of RTD, at all times during the performance of this **Contract**, the **Contractor**, subcontractor, vendor, supplier or third-party shall have and maintain a Cyber Risk Insurance policy. This

insurance shall be maintained for the duration of the **Contract** and a minimum of (2) two years following completion of the **Contract** with minimum limits of liability as follows.

Amount of Coverage:	$5,000,000 per occurrence $5,000,000 aggregate

The policy shall include the following types of coverage:

Security Breach – Liability
Network Security & Privacy
Media Liability
Regulatory Defense & Penalties
Privacy Breach Costs
PCI Fines and Penalties
Data Restoration Costs and Expenses
Network Business Interruption
Cyber Extortion and Terrorism
Security Breach Expense
Public Relations
Business Income and Extra Expense
Employee Privacy Liability

Endorsements, Waivers and Related Requirements

Prior to performing any Work, the **Contractor** shall furnish RTD with proof of insurance and a certificate of insurance for each of the **Contractor's** and each of its subcontractors' policies. All insurance policies required hereunder shall contain or be endorsed to contain the following provisions:

1. The **Contractor** and its subcontractors shall request their insurance policies contain language requiring the insurer to provide RTD with 30 days' advance notice of cancellation of policies by Registered or Certified mail. Regardless, the **Contractor** and its subcontractors shall be responsible to immediately notify RTD in writing by email of any changes to, cancelations of or notices of an insurer's intent to not renew its insurance. Such notice shall be provided no later than 24 hours after the **Contractor** or any of its subcontractors receives notice of any changes, cancellations or notice of an insurer's intent to not renew. Failure to provide the notice shall be breach of the **Contract** and the **Contract** may be terminated. Any notice of changes, cancellation or intent to not renew shall be provided to the designated RTD Department or Division as provided herein. Such notice requirement does not waive the insurance requirements contained herein.

2. For the insurance specified herein, RTD and its members, directors, officers, employees and agents shall be named as an additional insured (except Workers' Compensation). Coverage shall be provided by Forms CG 2038 (ongoing operations) and CG 2040 (completed operations) or by an alternative endorsement approved by RTD.
3. For the insurance specified herein, the **Contractor's** and its subcontractors' insurance shall be primary and non-contributory insurance with respect to the **Contractor's** and its

subcontractors' insurance for RTD and its members, directors, officers, employees and agents. **Contractor** and subcontractor policy/policies shall contain ISO Form 2001 04 13, or such other form or endorsement approved by RTD.

4. The insurance specified herein shall contain an express waiver of subrogation in favor of RTD as by ISO form CG 2453 or CG 2404. The **Contractor** and its subcontractors and their agents and employees waive all rights of subrogation against RTD for any liability and workers' compensation claims they incur in relation to the **Contract** and agree to have all such policies appropriately endorsed with a Waiver of Subrogation endorsement.

5. The insurance shall apply separately to each insured and additional insured party against whom a claim is made or suit is brought, except with respect to the limits of the insurer's liability.

6. The amount of insurance must be **at least** equal to the limits of liability required herein.

Acceptable Insurance Company

The insurance company providing any of the insurance coverage required herein shall have at a minimum an AM Best Key Rating of A, with a Financial Strength of VII or higher, (i.e., A VII, A VIII, A IX, A X, etc.) or equivalent from similar rating agency and shall be subject to prior approval by RTD. Each insurance company's rating as shown in the latest AM Best Key Rating Guide shall be fully disclosed and entered on the required certificate of insurance.

Premiums, Deductibles and Self-Insured Retentions

The **Contractor** and its subcontractors shall be responsible for payment of premiums for all of the insurance coverages required hereunder. The **Contractor** and its subcontractors further agree that for each claim, suit or action made against insurance provided hereunder, with respect to all matters for which the **Contractor** and its subcontractors are responsible hereunder, the **Contractor** and its subcontractors shall be solely responsible for all deductibles and self-insured retentions. Any deductibles or self-insured retentions over $25,000 in the **Contractor's** and its subcontractors' insurance must be declared and approved in writing by RTD prior to entry upon, above or adjacent to RTD property and prior to commencement of any Work under the **Contract**.

.

Certificate of Insurance

The **Contractor** will deliver to the designated RTD Department or Division a certificate of insurance with respect to each required policy to be provided by the **Contractor** and its subcontractors. The required certificates must be signed by the authorized broker or agent representative of the insurance company shown on the certificate and authorized to bind the named underwriter(s) and their company to the coverage, limits and termination provisions shown thereon. All endorsements, waivers, and related requirements described above shall be attached to the certificates of insurance when submitted to RTD. A certified, true and exact copy

of each insurance policy (including renewal policies) required under this **Contract** shall be provided to RTD if so requested within three (3) days.

Maintenance of Coverage and Renewal Policies

No less than 21 calendar days prior to the expiration date of any policy to be provided by the **Contractor** and its subcontractors, the **Contractor** shall promptly deliver to RTD proof of insurance required by the terms specified herein for at least the next twelve months after the expiration date of any policy. Such insurance may be either a renewal policy or a new policy or policies.

No Recourse

There shall be no recourse by any party, insurer, the **Contractor** or its subcontractors against RTD for the payment of premiums, deductibles, self-insured retentions or other amounts with respect to the insurance required from the **Contractor** or its subcontractors.

Failure to Provide or Maintain Insurance Coverages

The **Contractor's** failure to have or maintain, or failure to require its subcontractors to have or maintain, any of the insurance coverage required herein shall constitute a breach of the **Contract**. In addition to the remedies that RTD may have under the insurance specified herein, RTD may take whatever action is necessary to maintain the current policies in effect (including the payment of any premiums that may be due and owing by the **Contractor** or its subcontractors) or RTD may procure substitute insurance. The **Contractor** is responsible for any costs incurred by RTD in maintaining the insurance coverage required by the terms specified herein or providing substitute insurance. Such costs may be charged to the **Contractor** or may be deducted from any sums due and owing to the **Contractor**.

BOND REQUIREMENTS

None required.

EXHIBIT 3—SPECIAL PROVISIONS/ALTERATIONS

SPECIAL TERMS

The following provisions have been specifically negotiated for this Contract and shall supersede to the extent that they conflict with corresponding provisions contained in Section III, Terms and Conditions, or any other conflicting requirements in the Contract Documents.

NONE

DELETED ARTICLES

The following provisions are deleted in their entirety from Section III, Terms and Conditions:

NONE

EXHIBIT 4

COMPLETED CERTIFICATIONS

SECTION IV ATTACHMENTS

ATTACHMENTS TO CONTRACT NO. 122DH059

Website Redesign

The following attachments contain material representations upon which the Contractor was selected for award of the Contract. These attachments form a part of the Contract Documents and are stored in the Contract file. Each of these attachments is incorporated in the Contract by this reference.

1. Request For Proposals Instructions
2. RFP Addenda
3. Contractor Submissions in Response to Request for Proposals
    a. Technical Proposal
    b. Cost Proposal
    c. Any Supplemental Information Utilized in Evaluating Award
4. Contractor Agreements, if any, Executed in Connection With the Contract