



PART H - EXHIBIT H – INFORMATION TECHNOLOGY TERMS AND CONDITIONS

1. General Overview:

This Information Technology Exhibit ("IT Exhibit") sets forth additional terms and conditions that apply to the Contractor's provision of information technology products or services under the Contract, including software, hosting or cloud services, system implementation, integration, maintenance, support, and any access to, processing of, storage of, or transmission of City Data. This IT Exhibit addresses, among other matters, service level expectations (if applicable), data ownership and use, cybersecurity and incident response, digital accessibility, subcontractor/third-party hosting requirements, records and audit rights, and transition assistance

2. Relationship to IT Exhibit

If the Scope of Work involves access to City information systems or City Data, the Information Technology Terms and Conditions set forth in Exhibit H are incorporated by reference and shall apply. In the event of a conflict, the IT Exhibit shall govern with respect to data protection, security, and information technology matters.

3. Applicability

This Exhibit applies only to the extent the Scope of Work includes information technology–related services, including but not limited to software, cloud-based services, system integration, data processing, hosting, maintenance, support, or technology-enabled professional services.

This Exhibit applies **only** to Contracts in which the Contractor will:

- access City information systems;
- store, process, transmit, or host City data; or
- provide software, cloud-based services, or technology-enabled services.

Nothing in this section shall be construed to expand or limit the City's rights or the Contractor's obligations beyond those expressly set forth in the Contract Documents.

4. Definitions (Excerpt from Part H, Exhibit A Definitions)

City Data –

Any data, information, records, content, or materials that are provided by or on behalf of the City, generated, collected, processed, stored, transmitted, or maintained for the City, or derived from the foregoing, in any form or media, including: (i) data and records created or received in the performance of the Contract; (ii) metadata and system logs to the extent



they contain City information; and (iii) any copies, extracts, backups, or archival versions of such data. City Data includes any Confidential Information of the City and any Personal Information to the extent present in the data.

Security Incident –

Any actual or reasonably suspected event that compromises, or reasonably threatens to compromise, the confidentiality, integrity, or availability of City Data or the City's information systems used in connection with the Contract, including: (i) unauthorized access to, acquisition of, use of, disclosure of, alteration of, or destruction of City Data; (ii) loss of control of credentials or access keys that could permit unauthorized access; (iii) malware, ransomware, denial-of-service attacks, or other exploitation affecting systems that store/process City Data; or (iv) any other incident that triggers notice or response obligations under applicable law.

Personal Information –

Information that identifies or can reasonably be used to identify an individual, alone or in combination with other information, including any information defined as "personal information," "personally identifiable information," or similar terms under applicable federal or Virginia law. Personal Information includes, at a minimum: name; address; telephone number; email address; date of birth; government-issued identification numbers (e.g., Social Security number, driver's license number); financial account numbers; health or medical information; biometric identifiers; geolocation data; online identifiers; and any unique identifier linked or reasonably linkable to an individual.

5. Service Levels and Performance Standards (If Applicable)

Where the Contract involves ongoing or recurring technology services, the Contractor shall perform such services in accordance with the service levels, performance standards, response times, or availability requirements expressly set forth in the Scope of Work or applicable Exhibit.

Failure to meet any Service Level shall be addressed in accordance with the remedies, credits, cure rights, and other enforcement provisions set forth in the Contract Documents and applicable law, and shall not limit or waive any other rights or remedies available to the City.

6. Key Personnel (If Applicable)

The Contractor shall not remove or replace any key personnel identified in its response without the City's prior written approval. Any approved replacement shall possess qualifications and experience substantially equivalent to those of the personnel being replaced.

This requirement applies only to personnel expressly identified as key personnel in the Contract or incorporated solicitation response materials.



7. Data Ownership

All data, records, files, and information created, received, maintained, or processed by the Contractor on behalf of the City in connection with the Contract ("City Data") are and shall remain the exclusive property of the City.

The Contractor acquires no ownership interest in City Data and may use City Data solely to perform its obligations under the Contract.

8. Custom Work Product:

To the extent the Contractor develops custom deliverables specifically for the City under the Contract, such deliverables shall be considered works made for hire to the extent permitted by law. To the extent any such deliverables are not deemed works made for hire, the Contractor grants the City a perpetual, non-exclusive, royalty-free license to use, reproduce, and modify such deliverables for governmental purposes.

This provision does not apply to pre-existing software, tools, platforms, or materials of the Contractor, which shall remain subject to the applicable license terms.

9. Data Security

The Contractor shall implement and maintain reasonable administrative, technical, and physical safeguards designed to protect City Data from unauthorized access, disclosure, alteration, or destruction.

Security controls shall be appropriate to the nature of the services provided and the sensitivity of the City Data involved.

Such safeguards shall be designed to meet any minimum requirements imposed by applicable Virginia law for the protection of personal information.

10. Unauthorized Access and Security Incidents

The Contractor shall promptly notify the City, in writing, **within 24 hours**, and in no event later than the timeframe required by applicable Virginia law, of any known or reasonably suspected unauthorized access, **disclosure, or security incident** involving City Data.

Such notice shall include, to the extent known at the time:

- a description of the incident;
- the categories of City Data affected; and
- the corrective actions taken or planned.



The Contractor shall cooperate with the City in responding to and mitigating the effects of any such incident, including supporting any required notifications to affected individuals, regulatory authorities, or law enforcement, as applicable. The Contractor shall not make any external notification or public statement regarding a security incident involving City Data without the City's prior written approval, unless otherwise required by law.

11. Compliance with Law

The Contractor shall comply with all applicable federal, state, and local laws and regulations relating to data protection, privacy, and information security in the performance of the Contract, including, where applicable, the Virginia Information Technology Access Act (Title 2.2, Chapter 35; §§ 2.2-3500 et seq.). and laws governing the protection of personal information.

12. Digital Accessibility (Required)

To the extent the Contract involves the provision of information and communication technology, including software, websites, applications, digital documents, or technology-enabled services made available to City employees or the public, the Contractor shall ensure such technology complies with applicable accessibility requirements under Virginia and Federal law. Including, but not limited to ADA Title II (WCAG 2.1 Level AA standard).

Upon request, the Contractor shall provide information reasonably necessary to demonstrate such compliance.

13. Subcontractors and Third-Party Hosting

The Contractor shall not permit any subcontractor or third-party service provider to access City Data unless:

- such access is necessary for Contract performance; and
- the subcontractor or third party is subject to data protection obligations no less restrictive than those set forth in this Exhibit.

The Contractor remains fully responsible for the acts and omissions of its subcontractors and third-party providers.

14. Return or Destruction of Data

Upon expiration or termination of the Contract, or upon the City's written request, the Contractor shall:



- return all City Data to the City in a commercially reasonable format, or
- securely destroy such data,

as directed by the City, unless retention is otherwise required by law , subject to applicable records retention requirements.

15. Audit and Verification

Upon reasonable notice and during normal business hours, the City may request information reasonably necessary to verify the Contractor's compliance with the obligations set forth in this Exhibit.

Nothing in this section shall be construed to require disclosure of proprietary or confidential security information beyond what is reasonably necessary for verification.

16. Freedom of Information Act and Proprietary Information

Records relating to this Contract may be subject to disclosure under the Virginia Freedom of Information Act. Any proprietary or confidential information submitted by the Contractor shall be clearly identified and marked at the time of submission. The City makes no guarantee that such information will be exempt from disclosure and shall handle all requests in accordance with applicable law.

17. Transition Assistance

Upon expiration or termination of the Contract, the Contractor shall, at the City's request and for a reasonable period of time, cooperate in the orderly transition of services to the City or a successor contractor. Transition assistance may include reasonable knowledge transfer, documentation, coordination, and cooperation necessary to minimize disruption to City operations.

Any transition assistance beyond the original Scope of Work shall be subject to mutual written agreement, including scope and compensation, if applicable.

18. Survival

The obligations set forth in this Exhibit shall survive expiration or termination of the Contract to the extent necessary to protect City Data and enforce the City's rights.