

**IT Contract Clauses
for
Washington State Agencies**

*Dated September 3, 2025*

# IT Contract Clause Guidance

This document is intended to provide guidance to State contracting officials on information technology related contract clauses. Historically the state relied on WaTech policy 141.10. WaTech has refined the IT policies and standards to replace policy 141.10. This document is intended to provide guidance for meeting those policies and standards in contracts. The contract language included here is provided as template language that agencies are free to change for their use case.

For assistance on using these clauses contact ContractsLiaison@des.wa.gov. The use of these contract clauses is based on the details of contract use. For IT clauses there is no one size fits all clause template. Use of clauses depends on the specific IT hardware, software, or service use case, initial guidance is provided in the Guidance chart on page 3. For individual clauses refer to the table of contents below.

Table of Contents

[IT Contract Clause Guidance 2](#_Toc207784519)

[Guidance Chart 4](#_Toc207784520)

[High level generic 6](#_Toc207784521)

[High level list of policies and standards 6](#_Toc207784522)

[Payment structure for advanced payment 7](#_Toc207784523)

[Software license 7](#_Toc207784524)

[Software as a Service (SaaS) 7](#_Toc207784525)

[Configuration/Customization of Software 7](#_Toc207784526)

[Software support/maintenance subscription services 8](#_Toc207784527)

[IT Warranty 8](#_Toc207784528)

[General IT warranty 8](#_Toc207784529)

[Software warranty 8](#_Toc207784530)

[IT Remedy 10](#_Toc207784531)

[Confidential Information and Data 10](#_Toc207784532)

[Confidential information default 10](#_Toc207784533)

[Alternative for Confidentiality Information: Generic WaTech policy/RCW 11](#_Toc207784534)

[Alternative for Confidential information: defined in DSA 11](#_Toc207784535)

[Cloud Services Customer Data definition 11](#_Toc207784536)

[User data (includes agency owned derived data) addition to customer data 11](#_Toc207784537)

[Derived Data alternative for DSA 11](#_Toc207784538)

[Data Security 11](#_Toc207784539)

[Security Audit additional language 13](#_Toc207784540)

[Data Breach addition for security incident 13](#_Toc207784541)

[Network Access 14](#_Toc207784542)

[Data Ownership and Use 14](#_Toc207784543)

[Long form for category 3 and 4 data 14](#_Toc207784544)

[Simple Category 1 or 2 data use 15](#_Toc207784545)

[Data storage location 15](#_Toc207784546)

[Data access locations 16](#_Toc207784547)

[Data Encryption 16](#_Toc207784548)

[Long form 16](#_Toc207784549)

[Short form 16](#_Toc207784550)

[Accessibility 16](#_Toc207784551)

[General accessibility clause 16](#_Toc207784552)

[Alternative Accessibility 16](#_Toc207784553)

[Simple versions citing the standard 17](#_Toc207784554)

[Simple version for the guidelines cited in the standard 17](#_Toc207784555)

[Authentication 17](#_Toc207784556)

[Data Format 17](#_Toc207784557)

[IT Software potential terms 17](#_Toc207784558)

[Software Updates 17](#_Toc207784559)

[Transition 18](#_Toc207784560)

[Transition Alternative 18](#_Toc207784561)

[IT Services terms 19](#_Toc207784562)

[Professional services 19](#_Toc207784563)

[Hosted Services 19](#_Toc207784564)

[Cloud Service guarantee 20](#_Toc207784565)

[Geographical Data 23](#_Toc207784566)

[Geospatial Data 23](#_Toc207784567)

[Web Accessible Geospatial Data 24](#_Toc207784568)

[Hydrography Data 24](#_Toc207784569)

[Next Gen 9-1-1 (NG9-1-1) 24](#_Toc207784570)

[Acceptable Use 24](#_Toc207784571)

[Non-compliance with IT System and Service Acquisition Policy 24](#_Toc207784572)

[Conditional Acceptance of Website or Clickwrap Terms 24](#_Toc207784573)

[Intellectual Property 25](#_Toc207784574)

[Option 1 = full statement 25](#_Toc207784575)

[Option 2 = customized basis focus 26](#_Toc207784576)

[Option 3 = simplest 26](#_Toc207784577)

[AI Disclosure 26](#_Toc207784578)

[Alternatives for AI notification 26](#_Toc207784579)

[If concerned on data use for development and only allow public data to be used (should be rare based on the business need): 26](#_Toc207784580)

[Limitation of Liability 27](#_Toc207784581)

[Insurance 27](#_Toc207784582)

[Technology professional liability 27](#_Toc207784583)

[Cyber Risk Liability Insurance 28](#_Toc207784584)

## Guidance Chart

This guidance chart provides prompts that may trigger the use of specific IT contract language and the title of that applicable language (which is featured later in this document).

|  |  |
| --- | --- |
| Use Case | Relevant Clauses |
| All IT contracts | Non-compliance with IT System and Service Acquisition |
| Software |  |
| Software as a Service/Cloud solutions | IT Warranty: Software WarrantyIT RemedyCloud Services Customer Data definitionData SecurityData Ownership – long formData encryptionData Sharing Agreement (which may include the above topics)Intellectual PropertyIT Software: Software UpdatesIT Software: TransitionIT Service: Hosted ServicesCloud Service guaranteeCyber risk insurance |
| Interface with state network | IT WarrantyIT RemedyNetwork AccessAcceptable Use |
| [Category 2 data](https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf) - Sensitive Information Sensitive Information is information that may not be specifically protected from disclosure by law and is for official use only. This information is generally not released to the public unless specifically requested.  | Encryption of data in transit and at restCyber risk insurance |
| [Category 3+ data](https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf) - Confidential InformationConfidential information is information that agencies cannot release to the public. It is information that is specifically protected by either state or federal law, and is exempt from public disclosure. | Encryption of data in transit and at restConfidential InformationData SecurityData Ownership – long formData Sharing Agreement (which may include the above topics)Cyber risk insurance |
| On-premises – maintenance contract – Contractor has access to network and data | IT WarrantyIT RemedyNetwork AccessAcceptable UseConfidential InformationData SecurityNetwork AccessData OwnershipIntellectual PropertyIT Software: Software Updates |
| Subscription services - annual software licenses- Contractor doesn’t have access to data | IT WarrantyIT Remedy |
| Perpetual license for software – off the shelf with no integration/configuration, Contractor doesn’t have access to data | IT WarrantyIT Remedy |
| Custom designed software – existing software development by consultant/Contractor(often called integration/configuration) | IT WarrantyIT RemedyEncryption of data in transit and at restConfidential InformationData SecurityData OwnershipIT Services: Professional ServicesTechnology Professional Liability |
| Requires authentication for users | Authentication |
| Network Set-ups-servers, VOIP, Telephony | IT WarrantyIT Remedy |
| Services |  |
| Consulting with network access | Network AccessAcceptable UseIT Services: Professional Services |
| Contractor service results in public records | Data FormatData Ownership and UseIntellectual Property |
| Consulting with access to [Category 2 data](https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf) - Sensitive Information Sensitive Information is information that may not be specifically protected from disclosure by law and is for official use only. This information is generally not released to the public unless specifically requested.  | Data Ownership and UseIntellectual PropertyAcceptable UseEncryption of data in transit and at restCyber risk insurance |
| Consulting with access to [Category 3+ data](https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf) - Confidential InformationConfidential information is information that agencies cannot release to the public. It is information that is specifically protected by either state or federal law, and is exempt from public disclosure. | Data Ownership and UseIntellectual PropertyAcceptable UseEncryption of data in transit and at restConfidential InformationData SecurityData Ownership – long formData Sharing Agreement (which may include the above topics)Cyber risk insurance |
| Other Goods and Services |  |
| IT goods/hardware with data storage | IT WarrantyIT Remedy |
| IT goods/hardware without data storageExample – IT Cabling/Switches | IT WarrantyIT Remedy |
| Goods/Services Contracts with no IT policy implications | None |

## High level generic

*Use Case: For when there are IT components in the solicitation/contract. While short, this generic approach is not clear to businesses on what the relevant policies and standards are and is not as complete as the more specific options. This may be sufficient for a simple contract where the policies and standards are clear to all parties. It is recommended to include the more robust provisions in this document for clarity to contractors because a common response to this approach from contractors is “describe what policies and standards apply to this Contract.”*

Contractor shall comply with applicable WaTech [policies and standards](https://watech.wa.gov/policies).

## High level list of policies and standards

*Use Case: For when there are IT components in the solicitation/contract and known applicable policies/standards. This is the list of standards under the WaTech IT Security category that were formerly policy 141.10. Remove the non-applicable standards based on the use case. This may be sufficient for a simple contract, where there are known use cases, it is recommended to include the more robust provisions in this document.*

Contractor shall comply with the following WaTech policies, standards, and guidance:

* SEC-02 - [Security Assessment and Authorization Policy](https://watech.wa.gov/policies/security-assessment-and-authorization-policy)
* SEC-03 - [IT Security and Privacy Awareness Training Policy](https://watech.wa.gov/policies/it-security-and-privacy-awareness-training-policy)
* SEC-04 - [Asset Management Policy](https://watech.wa.gov/policies/asset-management-policy)
* SEC-04-01-S - [Data Backup and Recovery Standard](https://watech.wa.gov/policies/data-backup-and-recovery-standard)
* SEC-04-02-S - [Media Sanitization and Disposal Standard](https://watech.wa.gov/policies/media-sanitization-and-disposal-standard)
* SEC-04-03-S - [Configuration Management Standard](https://watech.wa.gov/policies/configuration-management-standard)
* SEC-04-04-S - [Firewall Standard](https://watech.wa.gov/policies/firewall-standard)
* SEC-05 - [Change Management Policy](https://watech.wa.gov/policies/change-management-policy)
* SEC-06-02-S - [Remote Access Standard](https://watech.wa.gov/policies/remote-access-standard)
* SEC-07 - [Physical and Environmental Protection Policy](https://watech.wa.gov/policies/physical-and-environmental-protection-policy)
* SEC-08 - [Data Sharing Policy](https://watech.wa.gov/policies/data-sharing-policy)
* SEC-08-01-S - [Data Classification Standard](https://watech.wa.gov/policies/data-classification-standard)
* SEC-08-02-S - [Encryption Standard](https://watech.wa.gov/policies/encryption-standard)
* SEC-09 - [IT Security Audit and Accountability Policy](https://watech.wa.gov/policies/it-security-audit-and-accountability-policy)
* SEC-011 - [Information Security Risk Management Policy](https://watech.wa.gov/policies/information-security-risk-management-policy)
* SEC-11-01-S - [Risk Assessment Standard](https://watech.wa.gov/policies/risk-assessment-standard)
* SEC-11-02-S - [Vulnerability Management Standard](https://watech.wa.gov/policies/vulnerability-management-standard)
* SEC-04-01-G - [Media Handling and Data Disposal Best Practices](https://watech.wa.gov/policies/media-handling-and-data-disposal-best-practices)
* SEC-11-01-G - [Electronic Signature Guidelines](https://watech.wa.gov/policies/electronic-signature-guidelines)
* SEC-12 - [Information Technology Disaster Recovery Planning Policy](https://watech.wa.gov/policies/information-technology-disaster-recovery-planning-policy)
* SEC-13 - [International Travel Technology Policy](https://watech.wa.gov/policies/international-travel-technology-policy)
* SEC-13-01-S - [International Travel Technology Standard](https://watech.wa.gov/policies/international-travel-technology-standard)
* USER-02 - [Acceptable Use Policy](https://watech.wa.gov/policies/acceptable-use-policy)

## Payment structure for advanced payment

The Washington constitution, RCW 43.88, and OFM State Administrative & Accounting Manual prohibit advanced payments to Contractors in various ways. This can complicate payment structures for IT licenses and services.

### Software license

Licenses can be paid when receiving the software license as delivery of the good, in which case advanced payment is not an issue.

### Software as a Service (SaaS)

Paid as a subscription but functionally is a license delivered on day one since the software can be used to the full extent on the first day. Payment for the year when receiving the licenses would not be an advanced payment under OFM’s SAAM rules since the full use and benefits of the service begins on the day the licenses are active.

### Configuration/Customization of Software

Advanced payment on software can be a potential issue for configuration of software is a service paid once configuration is completed but can include partial payments for milestone in configuring the software. Example milestones: assignment of IP rights in the configuration, approved configuration plan, individual approved steps within the configuration plan, and final delivery.

Milestone language would modify the invoicing/payment section of the contract. Sample Language: Contractor shall invoice and receive payment from Agency based on the milestones listed below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Milestone | Detail | Approval | Date | Amount |
| Assignment of IP | The assignment of Intellectual Property rights in the customization of the software. This is value to the Agency since the Agency owns the IP rights to the customization. | Assignment document signed by both parties | by 2/1/20XX  | $100,000 |
| Configuration plan | The Contractors’ delivered details of the configuration to meet the Agency’s need. This is of value to the agency since it provides the complete project plan with more details on the deliverables. | Written approval by Agency | by 4/1/20XX | $150,000 |
| Phase 1 completion | The completion of phase 1 of the configuration plan that meets the Agency’s requirements.  | Completion of acceptance testing by Agency | by 7/1/20XX | $200,000 |

### Software support/maintenance subscription services

In the industry this subscription is paid for in advance to cover the support for that year. If treated as a service under OFM’s SAAM it would be paid at the end of the subscription. The contract could be structured to align with the prohibition on advance payment and reduce the Contractor’s risk, in part, by paying in arrears more frequently than annually (e.g., quarterly, monthly). This would be a different approach for the industry to comply with the advanced payment provisions.

Additional language for invoicing/payment section of the contract:

Contractor shall invoice Agency for support and maintenance services [quarterly/monthly/biweekly].

## IT Warranty

### General IT warranty

*Use Case: General warranty that covers many use cases. This is broad language of general applicability to IT use cases. Agencies may add or remove information based on the scope of the specific contract.*

Contractor warrants, that all hardware, software, and firmware associated with Services ( “IT Services”) will not: (a) contain any viruses, malicious code, Trojan horse, worm, time bomb, self-help code, back door, or other software code or routine designed to: (i) damage, destroy, or alter any software or hardware; (ii) reveal, damage, destroy, or alter any data; (iii) disable any computer program automatically; or (iv) permit unauthorized access to any software or hardware; (b) contain any third party software (including software that may be considered free software or open source software) that (i) may require any software to be published, accessed, or otherwise made available without the consent of Purchaser, or (ii) may require distribution, copying, or modification of any software free of charge; and (c) infringe on any patent, copyright, trademark, or other proprietary or intellectual property right of any third party or misappropriate any trade secret of any third party (“IT Warranty”). The IT Warranty will expire twelve (12) months after the date IT Services are complete, as applicable.

### Software warranty

*Use Case: For any IT software that has specifications as part of the contract/solicitation. This applies to SaaS, PaaS, and software hosted by the agency, either on the agency or WaTech servers.*

Current Version of Software and System Obsolescence. Contractor represents and warrants that it used the latest version of the SaaS/PaaS/software when developing the system for the Agency. Contractor represents and warrants that, except as provided in this section, the Software, hardware, equipment, and all other components of the System shall not become obsolete during the term of this Contract. Contractor’s pricing has included the cost of replacing obsolete software, hardware, and equipment through planned obsolescence by the applicable manufacturer and/or licensor. In the case that any such Software, hardware, or equipment becomes obsolete during the term of this Contract, Contractor will replace the affected components with functional equivalents that are subject to maintenance and support by the applicable manufacturer and/or licensor without additional cost to Agency.

System Functionality. Contractor represents and warrants that the operation of the System shall meet all Agency specifications as provided in this Contract and relevant exhibits and attachments following its acceptance by Agency. Contractor warrants that it will maintain the System to meet the standards set forth in this Contract. Contractor shall repair or replace any aspect or functionality of the System source code that does not meet applicable specifications as provided herein at no additional charge during configuration. Contractor also represents and warrants that the System will possess all the features and functions described in the documentation provided to Agency under this Contract and that the System will operate without any defects introduced or caused by the Contractor after a software upgrade or bug fix. Contractor shall immediately correct any System functionality that is not in compliance with such representations and warranties at no cost to Agency.

Contractor Performance. Contractor also represents and warrants that:

1. Contractor shall operate the System in a professional manner, with high quality, knowledge, and experience in business and systems integrations, maintenance, support, and operations.
2. Contractor shall perform all services required pursuant to the Contract in a professional manner, with high quality.
3. Contractor shall give highest priority to the performance of the System.
4. Time shall be of the essence in connection with performance of the System.
5. Contractor shall promptly and correctly re-perform services which are not in compliance with this Contract at no cost to Agency during configuration.
6. The System shall be available to Agency on a twenty-four hour, seven days a week basis at an uptime rate of 99.9% calculated monthly. “Available” means the System is with complete functionality and in accordance with the specifications set for in the Solicitation and Contract. The exemption to the availability would be during approved software maintenance and updates schedule approved by PURCHASER as described in the Contractor’s maintenance plan, as set forth in Exhibit H.

Ability to Perform. Contractor represents that it has and warrants that it shall have the capability and capacity to provide and operate the System it has agreed to provide to Agency, and that it shall secure all Third-Party Software licenses, if necessary, to operate the System in accordance with the terms of the Contract.

No Viruses/Malware. Contractor represents and warrants their cloud services do not contain any virus, ransomware, trap door, back door, time bomb, Trojan horse, worm, file infectors, or other malware. Should malicious code be identified during before or after deployment of the System, the Contractor must notify the AGENCY, remedy the issue, and provide what was done to remedy the issue to the AGENCY.

Agency Configurations. Any system configurations made by the Agency (either during testing or after acceptance) shall not void any warranties provided by Contractor in this Contract.

## IT Remedy

*Use Case: Include when using any warranty provision to cover what happens if a warranty is breached.*

IT Remedy. If IT Services do not comply with the IT Warranty, or if any defect or nonconformance develops during the IT Warranty Period, Contractor, at Agency’s election, promptly will: (a) re-perform or correct the non-conforming IT Services at no additional cost to Agency; or (b) refund the amounts paid for IT Services.

## Confidential Information and Data

### Confidential information default

*Use case: If the solicitation/contract includes confidential information. This is required for category 3 or 4 data from WaTech SEC-08, likely as part of a Data Sharing Agreement. This can be included for sensitive information for category 2 data.*

Confidential Information

1. Confidential Information. For purposes of this Contract, “Confidential Information” includes, but is not limited to, information that is deemed confidential under federal or state law, personal information as defined in [RCW 42.56.590](https://app.leg.wa.gov/RCW/default.aspx?cite=42.56.590), as well as any information identified, in writing, by Purchaser as confidential or protected.
2. Protection of Confidential Information. Notwithstanding any provision to the contrary, Contractor’s use of Confidential Information will be in compliance with all applicable state and federal law. At a minimum, Contractor shall maintain records documenting: (i) the Confidential Information received pertaining to this Contract; (ii) the purpose(s) for which the Confidential Information was received; (iii) who received and maintained the Confidential Information; and (iv) final disposition of the Confidential Information. Purchaser reserves the right to monitor, audit, and/or investigate Contractor’s use of Confidential Information used, collected, or acquired by Supplier pursuant to this Contract.
3. Contractor Obligation – Confidential Information. Contractor shall: (i) hold Confidential Information in strictest confidence and not make use of Confidential Information for any purpose other than the performance of this Contract; (ii) release Confidential Information only to authorized employees or agents requiring such information for the purpose of performing this Contract and who have executed an appropriate nondisclosure agreement or data sharing agreement as approved by Purchaser; (iii) implement and maintain physical, electronic, and managerial safeguards to prevent unauthorized access to Confidential Information including, but not limited to, storing Confidential Information on secure servers with access to the data strictly controlled and limited to staff with appropriate training and clearance; and (iv) ensure that all Confidential Information is encrypted in transmission from and to Contractor, at rest in the data base or other data facility maintained or used by Contractor, and when transmitted to authorized recipients using NIST FIPS approved encryption for the confidentiality and integrity of data at rest and data in transit.
4. Contractor Obligation – Expiration or Termination. Upon expiration or termination of this Purchase Order, Contractor, at Purchaser’s direction, timely will: (i) Certify to Purchaser that all Confidential Information has been destroyed; or (ii) return all Confidential Information to Purchaser; or (iii) take whatever other actions Purchaser requires of Contractor to protect such Confidential Information.

### Alternative for Confidentiality Information: Generic WaTech policy/RCW

*Use case: Variant for use of confidential information that relies on RCW and WaTech policy, rather than a full explanation.*

Confidential information. Contractor shall comply with RCW 42.56 regarding the disclosure of Information under this Contract and WaTech Data Sharing Policy SEC-08 regarding protection of data.

### Alternative for Confidential information: defined in DSA

*Use case: For when confidential information is defined in a data sharing agreement or contract exhibit.*

Confidential Information. Confidential Information is as any information that is deemed confidential under state and federal law as well as any information identified by [Agency] in [Data Share Agreement or other Exhibit].

### Cloud Services Customer Data definition

*Use case: For cloud services or hosted services where agency data is in the Contractors software/system.*

Cloud service and hosted service customer data. “Customer Data” means any and all information, data, materials, works, expressions, or other content, including any that are (a) uploaded, submitted, posted, transferred, transmitted, or otherwise provided or made available by or on behalf of Purchaser or any Authorized User for processing by or through the Services, or (b) collected, downloaded, or otherwise received by Contractor or the Services for Purchaser or any Authorized User pursuant to this Contract or at the written request or instruction of Purchaser or such Authorized User. Customer Data includes all User Data, Derived Data, and Confidential Information.

### User data (includes agency owned derived data) in addition to customer data

*Use case: For when the state wants to own all data in the system for cloud services.*

User Data. “User Data" means any and all information reflecting the access or use of the Services by or on behalf of Agency or any Authorized User, including any end user profile-, visit-, session-, impression-, click through-, or click stream-data, and any Derived Data based on or derived from any of the foregoing.

### Derived Data alternative for DSA

*Use case: Derived data is part of the services. This alternative defines derived data and states the allowable uses of Derived Data are provided in a separate Data Share Agreement.*

Derived Data. “Derived Data” means new data sets and/or data element(s) resulting from the creation, generation, and/or processing of some or all of the Data and Confidential Information sent by Agency to the Contractor [and/or its Subgrantees/subcontractors] through aggregation, algorithmic manipulation, or other processes; provided, however, that the Derived Data cannot be reverse engineered, associated with, or otherwise linked (directly or indirectly) to Purchaser or the Customer Data and Confidential Information. Use of Derived Data is defined in the in [Data Share Agreement or other Exhibit].

## Data Security

*Use Case: When the Contractor has state data this category 3 or 4 data and should be kept confidential/secure.*

Data Security Requirements.

1. Security Compliance. Contractor is responsible for establishing an information security program and maintaining physical, technical, administrative, and organizational safeguards, that comply with: (a) applicable industry standards and guidelines; (b) American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC) 1; and (c) Washington Technology Solutions Standards located at [link].
2. Annual Security Certifications. Contractor will, at the commencement of this Contract and annually thereafter provide Agency the following reports and certifications: (a) AICPA Statement of Standards for Attestation Engagement (SSAE) No. 18 SOC 1 Type II fiscal year cycle audit report; (b) SOC 2 Type I report in accordance with AICPA AT 101; and (c) attestation that Contractor’s Services are in compliance with Washington IT Policies and Standards. Agency may accept, at its sole discretion, alterative reports, audits or reporting formats which Agency determines to be equivalent or better to the reports and certifications described herein.
3. Data Breach. Contractor must have an incident response process that follows National Institute of Standards and Technology (NIST) of Standards and Technology (NIST) standards and includes breach detection, breach notification and breach response. Upon discovery or reasonable belief of any access, destruction, loss, theft, use or disclosure of Agency’s Data by an unauthorized party (“Data Breach”), Contractor shall notify Agency by the fastest means available and also in writing. Contractor shall provide such notification within forty-eight (48) hours after Contractor reasonably believes there has been such a Data Breach. Contractor’s notification shall identify:
	* 1. The nature of the Data Breach;
		2. The Data accessed, used or disclosed;
		3. The person(s) who accessed, used, disclosed and/or received Data (if known);
		4. What Contractor has done or will do to quarantine and mitigate the Data Breach; and
		5. What corrective action Contractor has taken or will take to prevent future Data Breaches.

Contractor shall quarantine the Data Breach, ensure secure access to Data, and restore Services as needed to comply with terms and conditions of this Contract. Contractor shall conduct an investigation of the Data Breach and shall share the report of the investigation with Agency.

In the event of the Data Breach, Contractor agrees to comply with all applicable state and federal statutory provisions, including but not limited to RCW 19.255.010 and [RCW 42.56.590](https://app.leg.wa.gov/RCW/default.aspx?cite=42.56.590). Where notifications are required to the public or regulators, Contractor shall coordinate and cooperate with Agency in the development of a communication plan, and promptly and at no cost, provide advance copies of any notifications for Agency review before disseminating. If a Data Breach occurs and is found to be the result of Contractor’s acts, omissions or negligence, Contractor shall assume complete responsibility for notification of affected parties, and be liable for all associated costs incurred by Agency in responding to or recovering from the Data Breach.

In the event of a Data Breach that is likely impact multiple agencies, more than 10,000 citizens, involve nation-state actors, or likely to be in the public domain Contractor shall notify WaTech Office of CyberSecurity within forty-eight (48) hours after Contractor reasonably believes there has been such a Data Breach.

1. Technical Examination and Audit. Upon advance written request, Contractor agrees that Agency or its designated representative shall have reasonable access to Services purchased by Agency under this contract, its operational documentation, records and databases, including online inspections. The online inspection shall allow Agency, its authorized agents, or a mutually acceptable third party hired by Agency, to test that controls are in place and working as intended. Tests may include, but not be limited to, the following:
	* 1. Operating system/network vulnerability scans;
		2. Web application vulnerability scans;
		3. Database application vulnerability scans; and
		4. Any other scans to be performed by Agency or representatives on behalf of Agency.

Contractor shall allow Agency reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Contract and Agency’s Data, at no cost to Agency. After any significant Data loss, specific to data stored within the Services platform, or as a result of any disaster or catastrophic failure, Contractor will at its expense have an independent, industry-recognized third party perform an information security audit. This does not apply to data loss resulting from interruptions in the Services stemming from Agency’s computers, network hardware, internet connectivity, or other elements owned or controlled by Agency that are reasonably required to use Services. The audit results shall be shared with Agency within seven (7) days of Contractor’s receipt of such results. Upon Contractor receiving the results of the audit, Contractor will provide Agency with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Contract.

### Security Audit additional language

*Use case: Provides clarity on the purpose and extent of the audit for security purposes. Agencies may add to the language based on use case to cover the scope of an audit. These are changes to the last paragraph of (d) above.*

Audit. Contractor shall allow Agency reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Contract and Agency’s Data, at no cost to Agency. Such audits are intended to demonstrate compliance with data security standards adopted by the WaTech, DES, and/or Agency, with the understanding that at a minimum, any such audits must determine whether security policies and standards (including, without limitation, data security policies, procedures, and controls) are in place to ensure compliance with all data security requirements set forth herein and as required by state and federal law. To the extent that additional information not enumerated herein is needed to fulfill this purpose, Contractor agrees to use commercially reasonable efforts to provide such information promptly and at no cost to Agency, the State Auditor’s Office, or their agents and representatives.

### Data Breach addition for security incident

*Use case: Requires Contractors to provide updates regarding potential data security incidents even before a data breach is confirmed.*

Security Incident. Security Incident means the successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Any Security Incident may constitute a Data Breach under this Contract.

If the Contractor does not have full details about the Security Incident, it will report what information it has and provide full details within fifteen (15) business days of discovery. To the extent possible, the initial report must include:

1. The nature of the unauthorized use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;

2. A description of the types of Data and Confidential Information involved;

3. The investigative and remedial actions that the Contractor or its Subgrantee/subcontractor took and/or will take to prevent and mitigate harmful effects and protect against recurrence; and

4. Any details necessary for a determination of whether the Security Incident is a Data Breach which requires notification under RCW 19.255.010, RCW 42.56.590, or any other applicable Data Breach notification requirement; and

5. Any other information that the Contractor has which Agency requests.

The Contractor must also take all reasonable actions to mitigate the risk of loss related to the Data and Confidential Information and comply with any notification or other requirements imposed by applicable law or Agency.

## Network Access

*Use case: If the Contractor will access agency network/folders.*

Network Access. During its performance of this Contract, Contractor may be granted access to Purchaser’s computer and telecommunication networks (“Networks”). As a condition of Network use, Contractor shall: (a) use the Networks in compliance with all applicable laws, rules, and regulations; (b) use software, protocols, and procedures as directed by Purchaser to access and use the Networks; (c) only access Network locations made available to Contractor by Purchaser; (d) not interfere with or disrupt other users of the Networks; (e) assure the transmissions over the Networks by Contractor (i) do not contain any libelous, defamatory, profane, offensive, obscene, pornographic, or unlawful material, and (ii) are not used to perform any illegal activities, including but not limited to, encouraging, selling, or soliciting illegal drugs, gambling, pornography, prostitution, robbery, spreading computer worms or viruses, hacking into computer systems, or trafficking credit card codes; and (f) upon termination or expiration of the Contract, relinquish all IP addresses or address blocks assigned to them on the Networks. Additionally, Contractor shall comply with Purchaser’s IT policies.

## Data Ownership and Use

### Long form for category 3 and 4 data

*Use Case: If the Contractor has access to category 3 or 4 data.*

Data Ownership, Use, Recovery.

1. Data Ownership and Use. Agency data (“Data”) shall include data collected, used, processed, stored, or generate as the result of the use of the Services. Data is and shall remain the sole and exclusive property of Agency. Contractor is provided a limited, non-exclusive license to access and use Data solely for performing its obligations under the Contract. Contractor shall: (a) keep and maintain Data in strict confidence and as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) not use, sell, rent, transfer, distribute, or otherwise disclose or make available Data for Contractor’s own purposes or for the benefit of anyone other than Agency without Agency’s prior written consent; and (c) not store, use, and transmit agency Data outside of the United States.
2. Encryption. Contractor shall use NIST FIPS approved encryption for the confidentiality and integrity of data at rest and data in transit. Contractors will maintain any validation or attestation reports that the encryption product creates. Any reports are subject to Agency’s audit in accordance with this Contract.
3. Data Backup. As part of the Services, Contractor is responsible for maintaining a backup of Data and for an orderly and timely recovery of such Data in the event that the Services may be interrupted. Contractor shall maintain a contemporaneous backup of Data that can be recovered within two (2) hours at any point in time. Use of remote services requires pre-approval by Agency’s Chief Information Security Officer.
4. Extraction of Data. Contractor shall, within one (1) business day of Agency’s request, provide Agency, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of the Data in the format specified by Agency.
5. Disaster Recovery. In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, Contractor shall notify Agency by the fastest means available and also in writing. Contractor shall provide such notification within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contactor shall inform Agency of: (a) The scale and quantity of the Data loss; (b) What Contractor has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and (c) What corrective action Contractor has taken or will take to prevent future Data loss. Contractor shall restore continuity of Services to meet the 24 hours Recovery Point Objective (RPO) and 72 hours Recovery Time Objective (RTO). At the commencement of the Contract, Contractor shall provide a copy of its disaster recovery plan and obtain Agency’s written approval of the disaster recovery plan. Contractor shall annually demonstrate the completion of disaster recovery testing and present a summary of test findings and any resulting remedial actions.

### Simple Category 1 or 2 data use

*Use Case: If the Contractor has access to category 1 or 2 data and no access to category 3 or 4 data.*

Data Ownership and Use. Agency’s data (“Data”) shall include data collected, used, processed, stored, or generate as the result of the use of the Services. Data is and shall remain the sole and exclusive property of Agency. Contractor is provided a limited, non-exclusive license to access and use Data solely for performing its obligations under the Contract. Contractor shall: (a) keep and maintain Data in strict confidence and as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) not use, sell, rent, transfer, distribute, or otherwise disclose or make available Data for Contractor’s own purposes or for the benefit of anyone other than Agency without Agency’ prior written consent; and (c) not store, use, and transmit agency Data outside of the United States; and (d) use NIST FIPS approved encryption for the confidentiality and integrity of Data at rest and Data in transit.

### Data storage location

*Use Case: explicit stating that data must be stored in the United States. This language is already included in long form(a).*

Offshoring of Software and Data. Contractor warrants that the system application solution and the storage of Agency Data will be hosted in the United States. No offshoring or offshore access of the system application solution or Agency Data is allowed.

### Data access locations

*Use Case: explicit stating that any data access must be stored in the United States. This is for any contract with Contractor provided services/maintenance where they have access to the data.*

Access to Data. Contractor agents who provide technical or customer assistance shall also be based within the United States if such technical or customer assistance could allow access to Agency Data.

## Data Encryption

### Long form

*Use Case: If the Contractor has access to category 3 or 4 data.*

Data Encryption. Contractor shall encrypt Agency Data at rest using encryption algorithms from FIPS 140-3 Security Requirements for Cryptographic Modules encryption algorithms in such a way that the data becomes unusable to anyone but authorized personnel.
Contractor shall encrypt Agency Data while in transit such that: (a) All manipulations or transmissions of data during the exchange are secure; (b) If intercepted by unauthorized parties during transmission the data cannot be deciphered; (c) When necessary, confirmation is received when the intended recipient receives the data; (d) Appropriate encryption methods for data in transit include, but are not limited to: Transport Layer Security (TLS) 1.2 or later version or Secure Shell (SSH) 2.0 or later version; and (e) Clients and servers must be configured to support the strongest cipher suites possible. Ciphers that are not compliant with this standard must be disabled.
Contractor must protect the confidential process, encryption key or other means to decipher the information from unauthorized access.

### Short form

*Use Case: If the Contractor has access to category 3 or 4 data.*

Data Encryption. Contractor shall use NIST FIPS approved encryption for the confidentiality and integrity of data at rest and data in transit. Contractors will maintain any validation or attestation reports that the encryption product creates. Any reports are subject to Agency’s audit in accordance with this Contract.

## Accessibility

### General accessibility clause

*Use Case: If the deliverables of the contract are a covered technology of the WaTech accessibility policy.*

Accessibility. All of Contractors [covered technology](https://watech.wa.gov/policies/definition-terms-used-policies-and-reports#Covered_Technology) provided as part of this Contract must be accessible to and usable by individuals with disabilities, either directly or by supporting the use of assistive technology. Contractor shall, at a minimum, meet the minimum accessibility standard outlined in WaTech USER-01-01-S.

### Alternative Accessibility

*Use Case: If the deliverables of the contract are a covered technology of the WaTech accessibility policy.*

Digital Accessibility**.**  If this Contract includes the acquisition, procurement, development, modification, or enhancement of public-facing digital content or tools; including websites, applications, and media (Covered Technology), the following requirements shall apply:

All Covered Technology under this Contract must meet Level AA compliance with [Web Content Accessibility Guidelines (WCAG) 2.2](https://www.w3.org/TR/WCAG22/).

Contractor shall validate compliance with this requirement through either a third-party accessibility validation report, a Vendor Product Accessibility Template (VPAT), or compliance review documentation.

Should the Covered Technology under this Contract fail to meet the required compliance Level, the Contractor shall submit a remediation plan addressing all issues identified to the Agency Contact identified on the cover page of this Contract. Agency may immediately terminate this Contract by providing Contractor written notice if Contractor fails to timely remediate all issues identified.

Simple versions citing the standard
*Use Case: If the deliverables of the contract are a covered technology of the WaTech accessibility policy.*

Accessibility. Contractors will take reasonable efforts to comply with WaTech Standard USER-01-01-S - Minimum Accessibility Standard or equivalent.

Contractor will comply with WaTech policy USER-01 Accessibility Policy and USER-01-01-S Accessibility Standard.

### Simple version for the guidelines cited in the standard

*Use Case: If the deliverables of the contract are a covered technology of the WaTech accessibility policy.*

Accessibility. Contractor shall meet or exceed Level AA compliance with [Web Content Accessibility Guidelines (WCAG) 2.1](https://www.w3.org/TR/WCAG21/) for all covered technology provided as part of this Contract.

## Authentication

*Use Case: If the service will use the active directory for single sign on.*

Authentication. Contractor solution must utilize Enterprise Active Directory (EAD), SecureAccess Washington (SAW), and Transact Washington (TAW) or otherwise comply with [183.20.10 Identity Management/User Authentication Standard](https://watech.wa.gov/policies/identity-management-user-authentication-standards) for user authentication.

## Data Format

*Use Case: If the Contract deliverable will be a public record that must be in a specific format.*

Data Format. Contract shall make all Data generated by Contractor’s solution that would be reasonably considered as a public record under [RCW 42.56](https://apps.leg.wa.gov/rcw/default.aspx?cite=42.56) available in an open and readily usable format consistent with the Agency’s Open Data Plan.

## IT Software potential terms

### Software Updates

*Use case: When purchasing software this is customer-friendly language governing updates and upgrades to the software (especially for cloud services).*

Updates and Upgrades. Contractor shall provide and install regular updates, patches, bug/security fixes, etc. made available to all Contractor customers (“updates”) to underlying technologies. These updates are included in the licensing, maintenance, and support Deliverables that will be provided by Contractor, and there shall be no additional costs for such updates. Contractor shall notify the Agency of any Software or system updates during the term of this Contract. Updates shall not reduce the functionality of or degrade the System.

Contractor shall provide any upgrades/new versions to the underlying Software or System that are made available to all other Contractor customers. These upgrades/ new versions are included in the licensing, maintenance, and support Deliverables that will be provided by Contractor, and there shall be no additional costs for such upgrades/new version. Contractor shall notify the Agency of any Software or System upgrades during the term of this Contract Upgrades/new versions shall not reduce the functionality of or degrade the System.

### Transition

*Use Case: When the Contractor has Customer Data upon the termination of the contract that must be used in the continuation of the services.*

Transition Services. Contractor represents and warrants that, in the event this Contract is transitioned to another contractor (e.g., Contract expiration or termination), Contractor shall use commercially reasonable efforts to assist Procuring Agency for a period of sixty (60) days to effectuate a smooth transition to another contractor to minimize disruption of service and/or costs to the State of Washington.

Contractor shall reasonably cooperate with other parties in connection with all services and tasks to be delivered under the Contract, including without limitation any successor service provider to whom Agency’s Data is transferred in connection with the termination or expiration of the Contractor. Contractor shall assist Agency, at no cost, in exporting and extracting Agency’s Data, in a format usable without the use of the services and as agreed by Agency. Any needed extension of services shall be provided for at the same terms, conditions, provisions, and pricing of the Contract, including any amendments, then in effect.

The Contractor must maintain the confidentiality and security of Agency Data during provision of the transition services and thereafter as required by Agency.

### Transition Alternative

*Use case: For longer term SAAS uses where the Customer Data went through extensive configuration in the software and the transition is likely to require substantial effort to extract the data for a useful function with a different system. This is generally rare as extraction of data is usually a quick process.*

Transition Services. Contractor represents and warrants that, in the event this Contract is transitioned to another contractor (e.g., Contract expiration or termination), Contractor shall use commercially reasonable efforts to assist Procuring Agency for a period of sixty (60) days to effectuate a smooth transition to another contractor to minimize disruption of service and/or costs to the State of Washington.

Contractor shall at a minimum cooperate with other parties in connection with all services and tasks to be delivered under the Contract, including without limitation any successor service provider to whom Agency’s Data is transferred in connection with the termination or expiration of the Contract. Contractor shall assist Agency in exporting and extracting Agency’s Data, in a format usable without the use of the services and as agreed by Agency. Any needed extension of services or extensive configuration to extract Agency’s Data in a specialized non-standard format for transition shall be provided for at the same terms, conditions, provisions, and pricing of the Contract, including any amendments, then in effect.

The Contractor must maintain the confidentiality and security of Agency Data during provision of the transition services and thereafter as required by Agency.

## IT Services terms

### Professional services

*Use case: If professional services are included in the scope of purchased services where there are clear timeline/deliverables for work to be performed. This is a separate provision governing payment and holdback for the work product based on the timeline of work.*

Professional Services. The maximum cost for Professional Services Fees shall not exceed \_\_ dollars ($\_\_). The Professional Services will be performed by the Contractor in distinct Work Product phases. These phases and deliverable details are provided in [Exhibit \_\_ - Scope of Work].

The table below is a fixed Delivery Date schedule for [WORK PRODUCT No. 1] and a projected Delivery Date schedule for the remaining [Work Products 2 – 5]. Each subsequent Work Product submittal will contain an updated Delivery Date, which will provide fixed payment details for that Work Product and a projected Delivery Date for future Work Products. Each projected Delivery Date should be adjusted as the Project progresses to accurately reflect future Delivery Dates. All subsequent WP Delivery Dates will mirror the content contained within [Exhibit \_\_ - Scope of Work]. Compensation for Work Product will not occur until such Work Product is completed by Contractor. The Purchaser shall withhold 15 percent from each Work Product payment (“Holdback Funds”) until FINAL Acceptance of all Work Products by Purchaser.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Work Product Number | Work Product Phases | Delivery Date | Value | Holdback Amount for Each WP | Net Payment Amount |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| TOTAL |  |  |  |  |  |

The Agency shall withhold 15 percent from each payment (“Holdback Funds”) until final System Acceptance by the Agency. The Contractor will itemize their invoice by stating the full amount to pay minus the 15%. The Agency will pay the Holdback Funds upon final System Acceptance plus the receipt of an invoice for the applicable Holdback Funds amount due. All payments of Holdback Funds are subject to Agency’s exercise of its remedies herein and as provided under the law.

### Hosted Services

*Use case: For when the Contractor is hosting the services with hosting fees and support and maintenance fees. This clarifies the payment section of the contract.*

Annual Hosting/Use Fees and Maintenance & Support. The Annual Hosting/Use Fee for Year One is provided in the table below and shall not exceed \_\_ dollars ($\_\_) during the Term of this Contract. The Annual Hosting/Use Fee for Year One is due and payable upon \_\_\_. Contractor shall provide Agency Annual Support and Maintenance for the Term of the Contract at the cost indicated, and the Contractor shall not charge Agency any additional Annual Support and Maintenance costs during the Initial Term of the contract.

The anticipated total compensation for the Annual Hosting/Use Fee plus Maintenance and Support are set forth in the table below. The terms of the Annual Hosting/Use Fee, Annual Maintenance and Support are set forth in the Contract, Exhibit X – Maintenance & Support. Payments for the Annual Hosting/Use Fee plus Maintenance and Support shall be paid beginning on the anniversary of Agency’s Acceptance of Work Product Five (Implementation). Based on the schedule, it is anticipated that any Annual Hosting/Use Fee plus Maintenance and Support after the Initial term of the Contract will require an amendment to extend the Contract for such services.

|  |  |  |  |
| --- | --- | --- | --- |
| Year | Description | Annual Fee | Totals |
| 1 | Annual Hosting/Use FeeAnnual Support & Maintenance | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| 2 | Annual Hosting/Use FeeAnnual Support & Maintenance | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| 3 | Annual Hosting/Use FeeAnnual Support & Maintenance | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| 4 | Annual Hosting/Use FeeAnnual Support & Maintenance | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| 5 | Annual Hosting/Use FeeAnnual Support & Maintenance | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| TOTAL |  |  | \_\_\_\_\_\_\_\_\_\_ |

## Cloud Service guarantee

*Use Case: For cloud services contracts there should be an up-time service level warranty as a stand-alone agreement or as a part of the main contract or statement of work.*

Service Levels and Credits.

Availability Requirement. Contractor shall make the Subscription Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Subscription Services (each such calendar month, a "Service Period"), at least [99.999%/99.95%/[OTHER NUMBER]%] of the time, excluding only the time the Subscription Services are not Available solely as a result of one or more Exceptions (the "Availability Requirement"). "Available" means the Subscription Services are available and operable for access and use by Agency and its Authorized Users over the Internet in [full/material] conformity with the Specifications. "Availability" has a correlative meaning. The Subscription Services are not considered Available in the event of [any/a material] performance degradation or inoperability of the Subscription Services, in whole or in part.

Exceptions. No period of Subscription Service degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following ("Exceptions"):

Customer's or any of its Authorized Users' misuse of the Subscription Services;

failures of Customer's or its Authorized Users' internet connectivity;

internet or other network traffic problems other than problems arising in or from networks actually or required to be provided or controlled by Provider [or its Subcontractor];

[or] Customer's or any of its Authorized Users' failure to meet any minimum hardware or software requirements set forth in the Specifications[./; or]

[Scheduled Downtime as set forth in Section X.X.]

Scheduled Downtime. Contractor shall notify Agency at least 24 hours in advance of all scheduled outages of the Subscription Services in whole or in part ("Scheduled Downtime"). All such scheduled outages shall: (a) last no longer than one hour; (b) be scheduled between the hours of [NUMBER] a.m. and [NUMBER] a.m., [TIME ZONE/LOCATION] Time; and (c) occur no more frequently than [once/[OTHER FREQUENCY]] per [week/[OTHER PERIOD]]; provided that Contractor may request Agency’s approval for extensions of Scheduled Downtime above one hour[, which approval may [be granted in Agency’s sole discretion/not be unreasonably withheld or delayed]].

Service Availability Reports. [Within [30/[OTHER NUMBER]] days after the end of each Service Period/In real time simultaneously with the performance of the Subscription Services], Contractor shall provide to Agency a report describing the Availability and other performance of the Subscription Services during [that/the current] calendar month and the [calendar/contract] year-to-date as compared to the Availability Requirement and Specifications. The report shall be in electronic or such other form as Agency may approve in writing and shall include, at a minimum: (a) the actual performance of the Subscription Services relative to the Availability Requirement and Specifications; and (b) if Subscription Service performance has failed in any respect to meet or exceed the Availability Requirement or Specifications during the reporting period, a description in sufficient detail to inform Agency of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement and Specifications are fully met.

Remedies for Service Availability Failures. If the actual Availability of the Subscription Services is less than the Availability Requirement for any Service Period, such failure shall constitute a Service Error for which Contractor shall issue to Agency the corresponding service credits as set forth in [Exhibit B ("Service Availability Credits")].

If the actual Availability of the Subscription Services is less than the Availability Requirement in any [two/[OTHER NUMBER]] of [four/[OTHER NUMBER]] consecutive Service Periods, then, in addition to all other remedies available to Agency, Agency may terminate this Contract and/or [any/the applicable] Service Order on written notice to Contractor with no liability, obligation, or penalty to Agency by reason of such termination.

Any Service Availability Credits due under this Section [ ] will be applied as set forth in [Exhibit X].

EXHIBIT [X] - SERVICE LEVELS

Availability and Service Availability Credits

|  |  |  |
| --- | --- | --- |
| Required Availability Service Level | Calculation Formula | Service Availability Credits |
| Subscription Services shall be Available [99.9999/99.95/[OTHER NUMBER]]% of the time during each Service Period excluding periods Subscription Services are not Available due to an Exception.  | (Actual Uptime ÷ (Scheduled Uptime – Total Minutes in Service Period Subscription Services are not Available Due to an Exception)) x 100 = Percentage Uptime. | No Service Availability Credits will be given for any Service Period in which Percentage Uptime equals or exceeds the Availability Requirement.Agency shall be entitled to a Service Availability Credit of 10% of the Fees payable for Subscription Services provided during the Service Period for each 1% by which Percentage Uptime is less than the Availability Requirement, such credit not to exceed 100%. |

Support Requests

|  |  |
| --- | --- |
| Support Request Classification | Description:Any Service Error Comprising or Causing any of the Following Events or Effects  |
| Critical Service Error | Issue affecting entire system or single critical production function;System down or operating in materially degraded state;Data integrity at risk;Material financial impact;Declared a Critical Support Request by the Agency; orWidespread access interruptions. |
| High Service Error | Primary component failure that materially impairs its performance; orData entry or access is materially impaired on a limited basis. |
| Medium Service Error | Subscription Service is operating with minor issues that can be addressed with a work around. |
| Low Service Error | Request for assistance, information, or services that are routine in nature. |

Support Service Level Requirements and Credits

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Support Request Classification | Service Level Metric(Required Response Time) | Service Level Metric(Required Resolution Time) | Service Level Credits(For Failure to Respond to any Support Request Within the Corresponding Response Time) | Service Level Credits(For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time) |
| Critical Service Error | [NUMBER] hours | [NUMBER] hours | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [hour/[OTHER PERIOD]] or portion thereof that the corresponding Service Error is not responded to within the required response time. | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for the first additional [hour/[OTHER PERIOD]] or portion thereof that the corresponding Service Error remains un-Resolved, which amount shall thereafter double for each additional [NUMBER] hour increment. |
| High Service Error | [NUMBER] hours | [NUMBER] hours | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [hour/[OTHER PERIOD]] or portion thereof that the corresponding Service Error is not responded to within the required response time. | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [hour/[OTHER PERIOD]] or portion thereof that the corresponding Service Error remains un-Resolved. |
| Medium Service Error | [NUMBER] days | [NUMBER] days | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [hour/[OTHER PERIOD]] or portion thereof that the corresponding Service Error is not responded to within the required response time. | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [NUMBER] days thereafter or portion thereof that the corresponding Service Error remains un-Resolved.  |
| Low Service Error | [NUMBER] days | [NUMBER] days | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [hour/[OTHER PERIOD]] or portion thereof that the corresponding Service Error is not responded to within the required response time. | [NUMBER]% of the Fees for the month in which the initial Service Level Failure begins and [NUMBER]% of such monthly Fees for each additional [NUMBER] days thereafter or portion thereof that the corresponding Service Error remains un-Resolved. |

## Geographical Data

### Geospatial Data

*Use Case: Contract includes geospatial data.*

Geospatial Data. Contractor shall provide all location based data/databases, geospatial data, geographic information systems, and geospatial data exchanges consistent with the Federal Geographic Data Committee (FGDC) standards.

### Web Accessible Geospatial Data

*Use Case: Contract includes web accessible geospatial data.*

Geospatial Data. Contractors building web accessible geospatial services including cached, web-based map services or dynamic map services consistent with [DATA-02-04-S Web Mapping Services Publication Standard](https://watech.wa.gov/policies/web-mapping-services-publication-standard).

### Hydrography Data

*Use Case: Contract includes hydrography data.*

Hydrography Data. Contractor shall provide all surface water (hydrography) geospatial datasets consistent with the U.S. Geological Survey (USGS) National Hydrography Dataset (NHD) and use NHD Data Dictionary that provides common structure to promote data sharing.

### Next Gen 9-1-1 (NG9-1-1)

*Use Case: Contract uses next gen 911.*

Next Gen 9-1-1. Contractor shall use the latest NENA NG9-1-1 GIS Data Model Standard for data that is loaded in the Spatial Interface (SI) functions of the Emergency Services IP Network (ESInet). All compatible Public Safety Answering Point (PSAP) environments incorporate NG9-1-1 data integration standards and associated capabilities.

## Acceptable Use

*Use Case: If the Contractor has access to Agency IT assets or devices.*

Acceptable Use. Contractors shall comply with the state Acceptable Use Policy ([USER-02](https://watech.wa.gov/sites/default/files/2024-09/User-02%20Acceptable%20Use%20Policy.pdf)) and Mobile Device Usage Policy ([USER-03](https://watech.wa.gov/sites/default/files/2024-08/USER-03%20Mobile%20Device%20Usage%20Policy_0.pdf)) for any IT assets used in performance of the Contract. Any devices Contractor provides must comply with Non-Agency Issued Device Standard ([SEC-04-07-S](https://watech.wa.gov/sites/default/files/2024-08/SEC-04-07-S%20Non-Agency%20Issued%20Device%20Security%20Standard.pdf)).

## Non-compliance with IT System and Service Acquisition Policy

*Use Case: If the Contract is for a WaTech* [*covered technology*](https://watech.wa.gov/policies/definition-terms-used-policies-and-reports#Covered_Technology)*.*
Non-compliance with System and Service Acquisition Policy. Contractor found to be non-compliant with IT System and Service Acquisition Policy must develop and execute a corrective action plan as soon as Agency becomes aware of the lapse. Contractors failure to comply with the IT System and Service Acquisition Policy may be subject to suspension or termination of contractual agreements, denial of access to agency Information Assets, and/or other actions as deemed appropriate by the agency.

## Conditional Acceptance of Website or Clickwrap Terms

*Use Case: If the purchase is of commercial software that comes with website/clickwrap terms.*

Acceptance of Website or Clickwrap Terms. Contractor shall timely notify Agency of any website term changes related to the Goods/Services. Agency is not bound by any Contractor website term, clickwrap, policy, clause, or future unilateral contract change that:

1. Increase the cost of the software programs or services without a written amendment and/or a request from Agency for additional licenses/services/term allowed by the contract.
2. Would eliminate or degrade access, services, maintenance and support that Agency has already paid or committed without entitling Agency to a full refund and option to cancel the contract without penalty.
3. Violates Washington state law or requires Agency to keep Contractor documents confidential. Any injunction to prevent any public records request for Contractor documents will remain the sole responsibility of Contractor to acquire in a timely manner after a formal notice of the request has been provided by Agency.
4. Would allow Contractor to commercialize Agency data or allow Category 3 or 4 data as defined in the [WaTech Data Classification Standard](https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf) (SEC-08-01-S) to be stored, created, transmitted, processed or altered outside of the United States.
5. Would require Agency to indemnify Contractor or any third party or otherwise be responsible for their attorney’s fees, litigation, arbitration/mediation related expenses, or would hold a party harmless for direct damages against Agency.
6. Would require jurisdiction, choice of law, venue or arbitration to be located anywhere other than Washington State in the appropriate court or forum within Thurston County.
7. Would require Agency to pay any taxes based upon Contractor’s gross income or receipts.
8. Would disallow or charge for access to records regarding this Contract required by Agency or the Washington state auditor/legislative audit and review committee for any legal purpose for a period of six years after the Contract ends.

## Intellectual Property

*Use Case: When the contract is for a work product that is produced for the agency as part of the contract. This can include custom applications, designs, photos, videos, media, reports, guidance, and other things made specifically for the agency as part of the contract. This would not cover commercial off the shelf software and applications which would be the property of the Contractors.*

### Option 1 = full statement

Ownership and Use of Intellectual Property.

1. Prior Intellectual Property. Each party’s intellectual property existing prior to the date of the Contract shall remain the exclusive property of that party.
2. Materials. As used herein, “Materials” means all information in any format that includes, but is not limited to, data, reports, documents, pamphlets, advertisements, books, surveys, studies, computer programs, films, tapes, and sound reproductions.
3. Works For Hire. Contractor promptly shall disclose to Purchaser, all developments, including designs, ideas, computer programs, discoveries, inventions, or improvements thereto, whether patentable, copyrightable, or not, made by Contractor in the performance of this Contract. Unless otherwise provided, all Materials produced under this Contract shall be considered "works for hire" as defined by the U.S. Copyright Act and will be owned by Purchaser. Purchaser shall be considered the author of such Materials. If the Materials are not considered “works for hire” under the U.S. Copyright laws, Contractor hereby irrevocably assigns all right, title, and interest in such Materials, including all intellectual property rights, to Purchaser effective from the moment of creation of such Materials.
4. License for Materials that Incorporate Pre-Existing Intellectual Property. For Materials that are delivered under this Contract, but that incorporate pre-existing Materials not produced under this Contract, Contractor grants to Purchaser a nonexclusive, royalty-free, irrevocable license (with rights to sublicense others) in such Materials to translate, reproduce, distribute, prepare derivative works, publicly perform, and publicly display. Contractor warrants and represents that Contractor has all rights and permissions, including intellectual property rights, moral rights, and rights of publicity, necessary to grant such a license to Purchaser.

### Option 2 = customized basis focus

Intellectual Property. All intellectual property rights in all works or supplies provided under this Contract which are written or produced on a customized basis, including, without limitation, all future such rights when the said works are created, shall be owned by Purchaser and Contractor shall ensure that it executes all documents necessary to effect such ownership. Where Contractor provides existing intellectual property right protected material to the Purchaser under this Contract it shall disclose this to Purchaser, warrants it has the right to do so and shall fully indemnify and hold harmless against all loss or liability arising from any third party intellectual property rights claims arising both from such existing material and in relation to any such bespoke work. Except as provided above both parties retain ownership of their pre-existing intellectual property right protected material.

### Option 3 = simplest

Intellectual Property. Unless otherwise provided, all material produced under this Contract shall be considered "works for hire" as defined by the U.S. Copyright Act and will be owned by Purchaser.

## AI Disclosure

*Use Case: If the Contractor will be using Generative AI.*

Artificial Intelligence Disclosure. Contract must disclose to [Agency] the use of Generative AI in applications utilized on this Contract.

### Alternatives for AI notification

Artificial Intelligence Disclosure. Contractor must notify [Agency] if their solution or service includes, or makes available, any GenAI including Gen AI from third parties or subcontractors. Contractor must provide: the model name, product owner, product description, use case, and the intended information use for the GenAI included in Contractor’s services. [Agency] reserves the right to terminate any contract that presents an unacceptable level of risk to the Agency.

During the term of the contract, Contractor must notify the [Agency] in writing if their services or any work under this contract includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors. [Agency] reserves the right to terminate any contract that presents an unacceptable level of risk to the Agency.

### If concerned on data use for development and only allow public data to be used (should be rare based on the business need):

Artificial Intelligence Data Use. Contractor shall not use non-public data or information in any data inputs in development of the Generative AI system.

## Limitation of Liability

*Use case: SaaS or cloud service contractors will attempt to limit liability. The following is approved by AGO. The limits should be determined within reasonable limits to cover the risk of the use. SaaS contracts and other cloud provider agreements will almost always include a contractor-friendly cap on liability that is typically no higher than the cost of one-year of services (rarely, two). This is an industry standard. This limitation should not apply to the highest risk areas of potential damages—namely, to contractor IP violations and data breaches involving confidential information. Alternatively, purchasers could agree to a so-called “super-cap” for higher risk breaches like data breach, security incidents, or IP Warranty.*

Limitation of Liability. Contractor’s liability arising out of or related to this contract will not exceed the greater of: (a) the fees payable to provider pursuant to this contract for products and services provided during the year before the last event giving rise to the liability; or (b) $\_\_\_\_\_\_\_. The limit of liability in the preceding sentence is cumulative and not per-incident.

The Limitation of Liability does not apply to breach of Sections \_\_\_\_\_ [IP Warranty, Data Breach]. Contractor’s liability arising out of or related to breach of these sections will not exceed \_\_ times the limit of liability set forth in section Limitation of Liability.]

## Insurance

### Technology professional liability

*Used when: Contractor is providing custom built applications or services for the agency. This would not cover commercial off the shelf uses where there is no customization by the Contractor for the agency.*

*$ limits based on: the function of the software and impact on the agency.*

Technology Professional Liability & Cyber Liability Insurance. Contractor agrees to purchase and maintain throughout the term of this Contract a technology/professional liability insurance policy, including coverage for network security/data protection liability insurance (also called “cyber liability”) covering liabilities for financial loss resulting or arising from acts, errors, or omissions, in rendering technology/professional services or in connection with the specific services described in this Contract:

Violation or infringement of any right of privacy, including breach of security and breach of security/privacy laws, rules or regulations globally, now or hereinafter constituted or amended;

Data theft, damage, unauthorized disclosure, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally identifiable information or confidential information in whatever form, transmission of a computer virus or other type of malicious code; and participation in a denial of service attack on third party computer systems; Loss or denial of service; No cyber terrorism exclusion; with a minimum limit of $\_\_\_\_\_\_\_\_\_ each and every claim and in the aggregate. Such coverage must include technology/professional liability including breach of contract, privacy and security liability, privacy regulatory defense and payment of civil fines, payment of credit card provider penalties, and breach response costs (including without limitation, notification costs, forensics, credit protection services, call center services, identity theft protection services, and crisis management/public relations services).

Such insurance must explicitly address all of the foregoing without limitation if caused by an employee of Contractor or an independent contractor working on behalf of Contractor in performing services under this Contract. Policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world. Such insurance must include affirmative contractual liability coverage for the data breach indemnity in this Contract for all damages, defense costs, privacy regulatory civil fines and penalties, and reasonable and necessary data breach notification, forensics, credit protection services, public relations/crisis management, and other data breach mitigation services resulting from a breach of confidentiality or breach of security by or on behalf of Contractor.

### Cyber Risk Liability Insurance

*Used when: Contractor has access to: Sensitive state data, Personally Identifiable Information (PII), Personal Health Information (PHI) [HIPAA], Financial Information, Data protected by federal or state law, and/or Contractor processes or stores that data
$ limits based on: the extent of data covered and the category of data (PII costs an average of $150 per record in a breach). The average data breach in 2020 cost $3.86 million; government breaches are often higher with personal information and highest with personal health information.*

Cyber Risk Liability Insurance. Cyber risk insurance, on a claim form. This coverage shall include Contractual Liability insurance for the indemnity provided under this Contract. Limits are $\_\_\_\_\_\_\_\_\_\_ per occurrence and $\_\_\_\_\_\_\_\_\_\_ aggregate.