INSURANCE REQUIREMENTS
(CYBERLIABILITY)

General

Vendor must maintain, for the duration of the Agreement and three years following its termination or expiration, a policy of cyber security liability insurance coverage for any loss resulting from a data breach, security incident or potential compromise of data in accordance with the following schedule and requirements:

Tiered Coverage Schedule	
Number of PII records	Limits of cyber liability insurance required (occurrence = data breach)
1-10,000	$2,100,000 per occurrence
10,001 – 50,000	$3,200,000 per occurrence
50,001 – 100,000	$4,250,000 per occurrence
100,001 – 500,000	$16,000,000 per occurrence
500,001 – 1,000,000	$32,000,000 per occurrence
1,000,001 – 10,000,000	$106,000,000 per occurrence
"Personal Information" or "PII" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, other identifying numbers, and any financial identifiers.	

The insurance policy shall comply with all of the following requirements:

- Issued by an insurance company acceptable to the City of Everett (City) and in force for the entire term of the Agreement, inclusive of any term extension(s).
- Contain a liability limit no less than the **per occurrence** limit stated in the table above for the Vendor's maximum system City PII record count. (The table is based on the Ponemon Institute per record cost of a data breach in 2022.) The Vendor shall adjust coverage as necessary in accordance with the above table if record counts change
- Shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
- Must include coverage for:
    - Computer forensics assistance to assess the impact of a data breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with breach notification laws
    - Notification and call center services for individuals affected by a security incident, or privacy Breach credit monitoring

    - Breach resolution and mitigation services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identity theft assistance,
    - notification costs to data breach victims, and regulatory penalties and fines.
- Shall apply separately to each insured against whom claim is made or suit is brought, subject to the Vendor's limit of liability, if any.
- Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

Vendor Insurance Is Primary

Vendors insurance shall be primary with respect to the City, and any other insurance or self- insurance maintained by the City shall be excess and not contributing insurance with the Vendor's insurance.

Notice

There shall be no cancellation, material change, reduction in limits or intent not to renew the insurance coverage(s) without 30 days written notice from the Vendor or its insurer(s) to City.

Evidence of Insurance

Prior to commencement of the services, Vendor shall deliver to the City a Certificate of Insurance acceptable to the City meeting the requirements set forth above. The requirements contained herein, as well as any City s review of insurance maintained by Vendor, is not intended to and will not in any manner limit or qualify the liabilities or obligations assumed by Vendor under the Agreement

Termination

In the event Vendor fails to provide such evidence or to maintain the required insurance coverage, the City may, in addition to any other remedies it may have, terminate the Agreement.