# Attachment 14- Cyber Security Requirements

Please review the document and mark up as needed. Not all requirements will apply to all projects. The City will determine the coverage limits based on scope of project.

# INSURANCE LANGUAGE

Vendor/Consultant shall procure and maintain for the duration of the contract insurance against claims for security breaches, system failures, injuries to persons, damages to software, or damages to property (including computer equipment) which may arise from or in connection with the performance of the work hereunder by the Vendor, its agents, representatives, or employees. Vendor shall procure and maintain for the duration of the contract insurance claims arising out of their services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy and breach of data.

**Cyber Liability** Insurance, with limits not less than **$2,000,000** per occurrence or claim,

**$2,000,000** aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

## Technology Professional Liability Errors & Omissions

### (Include this section only if vendor is providing a technology service (data storage, website designers, etc.,) or product (software providers)

**Technology Professional Liability Errors and Omissions Insurance** appropriate to the Consultant’s profession and work hereunder, with limits not less than $2,000,000 per occurrence. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by the Vendor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

a. The Policy shall include, or be endorsed to include, ***property damage liability coverage*** for damage to, alteration of, loss of, or destruction of electronic data and/or information “property” of the Agency in the care, custody, or control of the Vendor. If not covered under the Vendor’s liability policy, such “property” coverage of the Agency may be endorsed onto the Vendor’s Cyber Liability Policy as covered property as follows:

If the Vendor maintains broader coverage and/or higher limits than the minimums shown above, the Entity requires and shall be entitled to the broader coverage and/or the higher limits maintained by the contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to the Entity.

**HOLD HARMLESS LANGUAGE**

For purposes of drafting hold harmless language and insurance requirements for contracts with third parties who may provide cyber and tech services, including data processing services to the City, the it is advised to consider the broadest possible indemnity, not limited to bodily injury or property damage but should specifically include wording that encompasses cyber- related risks that include theft, loss or misuse of data, release of private information and responsibility for costs, fines and penalties that the entity might incur.

Beyond that, questions should be asked about the contractor’s data security procedures, including whether or not they have been audited to industry standards regarding their controls over information technology and related processes.

**AGREEMENT/CONTRACT RECOMMENDATIONS**

In drafting the agreement, it is suggested that the following points be taken into consideration:

## Essential Privacy and Security Terms

Every contract with privacy and data security implications should contain certain defined terms. Organizations should push for definitions that align with the business objectives of the contract and encompass all data accessed or processed by the vendor.

* 1. **Personal Information** – Properly defining this term will ensure the vendor’s duties align with the organization’s obligation to protect personal information under state, federal and international law.
     1. If a vendor accesses, stores or processes any personal information, such as personally identifiable information (“PII”), protected health information (“PHI”), or payment card information (“PCI”), include these items in the definition to ensure it is specifically protected.

## Confidentiality

Standard contract language is often too narrow or omits provisions of confidentiality for information that is protected under state and federal law, which can result in disputes if it is unclear whether information that has been breached falls under the contract. Consider the following:

1. Make sure that the definition of Confidential Information is broad and applies to the relevant data or intellectual property the vendor collects, stores, or processes on your behalf. If the vendor collects any personal information, protected health information (“PHI”), or payment card information (PCI), include these items in the definition of confidential information to ensure confidential treatment of the same.
2. If the City is providing credentials to the vendor to access the network or systems, make sure that such credentials are deemed confidential information.
3. Require access to confidential information only on a “need to know” basis.
4. Require vendor to enter into similar confidentiality agreements with staff, third- parties, and subcontractors who may have access to confidential information.

## Data Protection Provisions

Clear and specific data protection provisions will allow the City to limit its exposure due to a vendor’s failure to employ standard security practices. The data protection provisions should apply to all vendor personnel, including contractors and subcontractors with access to data. Depending on the

relationship, the City may want to require that all vendor personnel agree to the data protection provisions in writing.

* 1. **Standard of Care** – It is important to establish a baseline standard of care for vendors to employ when accessing or processing the City’s information. Minimally, vendors should be expected to use the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination, or publication of the City information as it uses to protects its own, including standard anti-virus/malware deployment.
  2. **Information Security Program –** Consider requiring the vendor to have a written information security program in place.
     1. Entities that store or maintain PII, PCI, or PHI are required to implement reasonable security to safeguard information in their care. Vendors that do not have a written information security program or resists a contractual agreement requiring one, should be viewed skeptically.
     2. Consider requiring vendors of all sizes to conduct periodic penetration testing and/or risk assessments. Although not a requirement, periodic testing and risk assessment is a sign of information security maturity.
  3. **Notification of an Information Security Incident** – It is important that the contract require prompt notification in the event of an information security incident involving the City’s data. However, consider the timing and how quickly you will want to be notified.
     1. Faster is not always better. Forensic investigations take time to understand the full scope of the incident and identify potentially affected individuals. Most legal notification deadlines start from when the City is notified by the vendor. If the vendor notifies the City immediately, the clock will start running before the vendor has completed their investigation, further reducing the amount of time the City has to notify affected individuals. ***The City might want to consider a discussion on timing considerations for these types of contracts.***
     2. Consider requiring the vendor to notify the City of actual or suspected use, disclosure, or acquisition of your data by an unauthorized actor.

### The vendor may attempt to limit notice obligation only to “actual” incidents instead of encompassing “alleged” incidents – make sure you include language requiring notification for alleged as well

* 1. **Incident-Related Costs** – In the event that an incident occurred due to a failure of the vendor to secure the City’s data, consider shifting the City’s costs associated with investigating, addressing, and responding to an incident to the vendor. The threat of exposure to these costs may provide the vendor additional incentive to keep the City’s data secure.

## Compliance with Privacy Laws

It may be helpful to set out the privacy laws that the City organization expects its vendors to comply with. These are a few but may not apply to all contracts.

1. GLBA (financial), FCRA (consumer reports / HR data), CAN-SPAM (marketing)
2. PCI DSS – if handling payment card data
3. GDPR
4. HIPAA – if handling medical records or health information
5. FERPA – if handling student data
6. CCPA/CCPR or its equivalent
7. Certain states impose minimum security requirements (e.g. California, Illinois, Massachusetts, and New York

## Access to Systems

The principle of least privilege – only permitting a user to access data or systems that is necessary to perform their duties – is an important data risk management tool for organizations of all sizes. This principle can also be applied to vendors to help limit the City exposure in the event of a data security

incident. This City should always consider defining **where your data can be stored and what happens after the vendor no longer needs access**.

* 1. **Restrictions** – Depending on the scope of engagement, the City may consider the following restrictions for vendors who access or process the City’s data:
     1. Domestic Operations: No access or transfer of data to/from outside of the United States (domestic operations); international operations should be subject to the appropriate legal instrument(s) governing access or transfer.
     2. No modifications to the City’s data.
     3. No unauthorized access.
     4. Restrict access to those who “need to know” in order to perform services under the agreement.
     5. Require vendors to **terminate credentials** of an employee who no longer needs access to the City’s systems to perform their duties. Credential management is a best practice to help limit activity by disgruntled individuals or malicious actors.
  2. **Data Storage** – Limiting the data that can be stored outside of the City is an important data loss prevention tool. Consider the following:
     1. Limit the data that can be stored outside of your environment to that necessary for a vendor to perform services and authorized by your organization.
     2. Do not permit the storage of company data on vendor mobile/removable devices (e.g. laptops, USB drives, or removable) except for **limited purpose and duration**.
  3. **Data Destruction** – Consider requiring that vendors to destroy or securely return the City’s data upon termination or expiration of the engagement.

## Audit Rights

Trust, but verify. Depending on the size and nature of your contract, consider requiring vendors to submit to information security audits or questionnaires to ensure compliance with the requirements of the agreement. Below are a few audit considerations for your organization when negotiating vendor contracts.

* 1. Determine who will conduct the audit – vendor, third-party, or resources at the City.
  2. Decide on the scope and frequency of the audit as determined by the size and information accessed by the vendor.
     1. The less onerous the audit measure, the more frequently it can be requested.
        1. Penetration testing – monthly
        2. Risk Assessments – quarterly
        3. Full SOC 2, Type II, or ISO 27001 certification – yearly

## Indemnification and Limitation of Liability

Standard limitations on liability are most likely too low to cover the costs related to a breach as breaches often expose companies to significantly high costs for remediation and legal fees. If the vendor had more control over the factors giving rise to a particular risk, the vendor should bear more responsibility in the event that such risk materializes and results in damages to the City.

* 1. **Security breaches** – Where the vendor is likely responsible, include indemnity language for liability for security breaches and failure to timely notify thereof to vendor; indemnity should cover any breach of confidentiality and security obligations. Depending on who the laws see as the original data owner, the City may still have liability and may need to file suit against the vendor to draw upon their insurance policy, should the contractual language not indemnify the City to the fullest extent. The City should not only require that the vendor indemnify you, but also that the vendor cooperate with any pending litigation or investigation in connection with security incident.

## Carve-outs:

* + 1. Insist on exceptions to a limitation of liability cap in instances of gross negligence, willful misconduct, or fraud and in cases of third-party claims.
    2. Limitation of liability provisions should not disclaim the costs of termination and any additional costs the City may incur to obtain alternative functionality as promised in the original contract that vendor failed to deliver.
    3. Exclude breach of confidentiality, data security, notification and data privacy obligations from the limitation of liability provision to the greatest extent possible. If vendor will not exclude such claims, attempt to negotiate a separate liability cap.
  1. **Remedies** – Limitation of liability provisions should address specific remedies in the event of a breach, including liquidated damages, the right to seek injunctive relief, the right to terminate, credit for not meeting service levels, the release of materials from escrow, breach notification reimbursement, special damages for epidemic failure, etc.
  2. **Impact on Insurance** – If the City agrees to indemnify vendor against third-party claims, consult with Risk so that the question can be asked of the insurance broker to make sure your policy covers the claims and to understand the potential impact of such indemnification language on coverage in general.

## Warranties

Generally, vendors tend to disclaim all warranties unless specifically stated otherwise. It is therefore crucial to include affirmative, express warranties regarding security. Warranties should be tailored to match the specific services rendered.

* 1. Require vendor to provide warranties of adequate internal security standards and any such standard that specifically relate to the product acquired or services rendered.
  2. Require vendor to give ample prior notice of any material changes to the deliverables that could adversely affect security and/or data integrity.
  3. Vendor should represent that any work product should be free and clear of viruses.
  4. Vendor should provide proper documentation and/or user manuals describing the deliverable and technical specifications. Work product and all related equipment, software and systems should substantially conform with such documentation.

## Termination

The ability to terminate an agreement with a vendor who did not adhere to certain security standards or suffered a breach is essential to the protection of the City’s data. Even if a breach was not involved, the termination of a contract may present additional risk to the City because the vendor **may no longer be under any duty to protect the City’s confidential information.** Consider the following to award the City’s data maximum protection and to transition the engagement to another provider swiftly and effectively:

* 1. **Termination due to a security failure** – If termination for convenience cannot be agreed upon, reserve the right to terminate if vendor fails to comply with its security representations and obligations under the agreement (those do not have to amount to a full-blown breach).
  2. **Return of materials upon termination** – Vendor should return or destroy all data and materials provided to vendor or created by vendor in the course of the engagement. Sever access to any systems post-termination should be provided for.
  3. **Transition Assistance** – Require assistance if data or materials need to be transferred to a subsequent service provider.
  4. **No data “Lockout”** – Vendor should return data and materials regardless of any other open items and payment obligations; data should not be held “hostage.”

## Subcontractors and liability for third parties

When engaging a vendor who may use subcontractors to provide the contracted services, the City’s main objective is to hold the vendor to the same performance standards and liabilities regardless of who performs the work. Therefore, the vendor should require any subcontractors to meet the same security standards as vendor is required to meet. Key considerations include the following:

* 1. Vendor should be accountable and liable for any acts or omissions by third-parties (such as failure to employ adequate security measures) in accordance with any limitation of liabilities/indemnification provisions in the contract.
  2. **Permission to Subcontract** – Vendor should seek prior authorization to subcontract in writing. If vendor will not agree to prior written consent, vendor should at a minimum promptly notify you of any subcontracting. Vendor should not be permitted to subcontract services that access or process sensitive company information.
  3. **Access** - Make sure that third-party access rights are spelled out conspicuously to help control who has access to the data and how it can be used when multiple participants are involved.

## Preservation Notices and E-Discovery

Records, documents and communications with the vendor may become relevant if litigation is brought against the City due to a security incident. Consider adding language along the lines of the following to ensure in advance that the vendor complies with discovery requests to help avoid friction over this issue in the future.

* 1. It is beneficial to add language ensuring vendor’s compliance with a third-party legal hold notice in the event of litigation, any preservation notices and document requests.
  2. In instances where the vendor provides software/platform, vendor should allow the City to retain an archival copy of the most recently used version of the software and all documentation in the event that discovery requests call for electronically stored information in native format.

## Insurance

Provided at the beginning of this document.