Vendor Cybersecurity & Contract Language

Introduction

This document is intended as a starting point for organizations, especially counties and municipalities, to incorporate cybersecurity requirements into their procurement and acquisition process. These requirements are designed to help protect an organization's data, especially consumers' personal information, as it is processed, stored, or transmitted by vendors outside of your organization's direct control.

These requirements were inspired by the Department of Defense's Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, but have been tailored for smaller organizations and their risk profile.

This document has two sections. The first provides draft language to insert into a broader organizational Cybersecurity Policy. The highlighted word 'Organization' is intended to be replaced by the name of the specific organization. The second section provides the corresponding language to be inserted into future vendor contracts and is adopted from the language in the General Services Acquisition Manual (GSAM), Part 552.239-71.

Big Security for Small Business
http://www.smallbiz-bigsec.org

Policy

Roles and Responsibilities

1. Vendors shall:
    a. Provide adequate security on all information systems used to process, store, or transmit Organization data.
        I. Adequate security means the protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
        II. To provide adequate security, the Vendor shall develop, implement, maintain, and provide upon request a Cybersecurity Plan.
        III. The Cybersecurity Plan may be based an approved cybersecurity framework, including the NIST Cybersecurity Framework (CSF), the ISO 27000-series standards, or the Center for Internet Security (CIS) Controls, but shall cover, at a minimum, policies and procedures for the following areas, based on the NIST CSF:
            1. Identify
                a. Roles and responsibilities
                b. Legal and regulatory requirements
            2. Protect
                a. Account Management. Specifically, vendors shall:
                    i. Use administrator accounts according to the principles of least privilege and separation of duties
                    ii. Promptly revoke credentials upon separation
                b. Authentication and Password Management. Specifically, vendors shall:
                    i. Enable multi-factor authentication where possible
                    ii. Consider using a password manager
                c. User Training
                d. Data Backups and Disposal
                e. Incident Response Plan
                    i. Shall include notification to the Organization of incidents affecting Organization data
                f. Incident Recovery Plan

Roles and Responsibilities (continued):

g. Vulnerability Management Plan. Specifically, vendors shall:
    i. Enable automatic software updates where possible
    ii. Perform antivirus and antimalware scanning
    iii. Establish a vulnerability disclosure program (VDP)

3. Detect
    a. Execution of the Vulnerability Management Plan
4. Respond
    a. Execution of the Incident Response Plan
5. Recover
    a. Execution of the Incident Recovery Plan

IV. The Organization CISO is the approval authority for all waivers or exemptions to this requirement, following consultation with Privacy, Legal, and other business units as appropriate.

b. Submit a self-certification of compliance to the requirements of 1(a).

c. Cooperate with the Organization Auditor during compliance audits.

Compliance:

1. The Organization Auditor shall evaluate vendor cybersecurity efforts by comparing submitted self-certifications to actual practices. Vendors may submit appropriate third-party documentation of compliance in lieu of Organization Auditor inspection.

Sample Contract Language

Section X.

Cybersecurity Requirements for Information Technology Resources

A. General. The Vendor shall be responsible for information technology (IT) cybersecurity for all systems that process, store, or transmit Organization data, regardless of location. This section is applicable to all or any part of the contract that includes information technology resources or services for which the Vendor has physical or electronic access to Organization's data. The term information technology, as used in this Agreement, means any equipment, including telecommunications equipment that is used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information.

B. Cybersecurity Plan. The Vendor shall establish, implement, and maintain a Cybersecurity Plan. This plan shall describe the processes and procedures that will be followed to ensure the appropriate security of IT resources that are developed, processed, or used under this contract. The Vendor Cybersecurity Plan shall comply with applicable laws.

C. Submittal of Cybersecurity Plan Self-Certification. Within 30 calendar days after contract award, the Vendor shall submit a Cybersecurity Plan Self-Certification to the Organization for acceptance. This self-certification shall affirm the vendor has implemented the required Cybersecurity Plan and is in compliance with the requirements stated in this section. The self-certification shall be incorporated into the contract as a compliance document. The Vendor shall comply with the Cybersecurity Plan.

D. Training. The Vendor shall ensure that its employees performing under this contract receive annual cybersecurity training.

E. Audit. The Vendor shall afford Organization reasonable and timely access to the Vendor's and sub-vendor's facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location, not more than once annually, except that such access shall be granted at any time in case of a data breach affecting Organization. Access shall be provided to the extent required, in Organization's sole discretion, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability, and

confidentiality of Organization data or to the function of information technology systems operated on behalf of Organization, and to preserve evidence of computer crime. This information shall be available to the Organization upon request. In lieu of an annual audit, Vendor may provide to Organization written documentation of its compliance with the Cybersecurity Plan or the underlying frameworks documented therein, prepared by a third-party.

F. Subcontracts. The Vendor shall incorporate the substance of this section in all subcontracts that meet the conditions in paragraph (a) of this section.

G. Termination. Failure on the part of the Vendor to materially comply with the terms of this section may result in the termination of this contract following a 30-day opportunity for Vendor to cure, following written notice and a demand for assurances or specific performance of the Agreement