Guiding Principles to Improve Vendor Cyber Security Contract Requirements

Version 1

REAL ESTATE CYBER CONSORTIUM
(RECC)

REAL ESTATE
CYBER CONSORTIUM

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

Real Estate Cyber Consortium (RECC) ("Consortium") standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While the Consortium administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

The Consortium is a volunteer professional organization with no regulatory, licensing or enforcement power over its members or anyone else. The Consortium does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public because its works are not obligatory and because it does not monitor the use of them.

The Consortium disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. The Consortium disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. The Consortium does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, the Consortium is not undertaking to render professional or other services for or on behalf of any person or entity, nor is the Consortium undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

The Consortium has no power, nor does it undertake to police or enforce compliance with the contents of this document. The Consortium has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. The Consortium does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document should not be attributable to the Consortium and is solely the responsibility of the certifier or maker of the statement.

PRIVILEGED AND CONFIDENTIAL

Real Estate Cyber Consortium (RECC) ("Consortium") board members and contributor members ("Participants") are expected to ensure their participation and communications serve the procompetitive objectives identified by Consortium and do not violate the antitrust laws. Participants should focus discussions on Consortium's statement of articulated objectives.

This means that no activity or discussion at our meetings or other functions, or independent of our Consortium activities, may be engaged in for the purpose of bringing about any understanding or agreement among the Participants' activities that affects competition among the Participants including any of the following: (a) raising, stabilizing, or setting prices for products and/or services of the Participants; (b) regulating the nature or volume of products or services offered by the Participants; (c) allocating geographic markets or customers served by the Participant; (d) encouraging boycotts or unreasonably seeking to exclude specific entities and/or third-party vendors from the Consortium; or (e) otherwise restricting competition among the Participants and/or among third-party vendors.

In addition, Participants must not discuss or reveal any individual Participant's competitively-sensitive proprietary information, including any Participant's prices, margins, discounts, costs, capacity, inventory, sales, customer lists/customer contacts, future business plans, or bids for contracts.

GUIDING PRINCIPLES

IMPROVING VENDOR CYBER SECURITY CONTRACT REQUIREMENTS

Preamble:

The world has continued to become more and more interconnected through advances in communications technology. The Real Estate vertical continues to explore and take advantage of innovative and potentially disruptive technology to improve efficiency, customer amenities and experience, and open opportunities through access to previously unforeseen datasets and analytics.

As a counterbalance, Information Security drivers for continuous **Availability**, trustworthy **Integrity** of data and **Confidentiality** of personal and business data has become a Board level discussion around the backdrop of not only negative reputational and financial impacts, but in the case of Building Technology, the very real specter of impacts to life safety.

Intent:

Understanding that every organization has different drivers from strategy, to objectives, to risk tolerance, this document aims to provide guidelines derived from industry experts. Future revisions of this document is intended to include boilerplate language that serve as a legal contract framework.

Last Modified
7/11/2019

REAL ESTATE
CYBER CONSORTIUM

BEST PRACTICE GUIDELINES

1. **Vendor must attend to Owner's Information Security Requirements**
   Each organization should have their own cyber security requirements and expectations. This clause should reflect that In addition to any Standard Agreement, the Vendor will adhere to the Owner's Information Security Requirements as they may apply to the Vendor's Services (i.e. on premises, SaaS, etc…).

2. **All Data Belongs to the Owner**
   Regardless the type of system, it should be explicitly stated that any and all data created and produced should belong solely to the Real Estate Owner organization, and that in the event that the vendor/landlord relationship expires, the data will be provided to the owner organization in a form requested by the owner within a specified timeframe.

3. **Personally Identifiable Information (PII)**
   Reflective of the increasing stringency of legislation, organizations should describe the meaning of PII and other sensitive information, using specific examples related to the system in question, and require vendors to collect only the information that is necessary for the intended use of the system. Vendors shall protect such data commensurate with recommended encryption practices reflective of the sensitivity of the data. Vendors should be instructed that the information cannot be shared, nor merged into other datasets without the consent of the data owner. Additional language in this area should indicate the applicable laws which govern data collection and privacy, and compel the proper disposal of PII and other sensitive information.

4. **Breach and Vulnerability Notification**
   Organizations must require vendors (as well as subcontracted vendors under the named service provider) to notify the Real Estate organization of any confirmed or suspected system or data breach(es) within a specified time period. This notification should include physical security breaches (such as document loss), as well as loss of mobile media. The organization should require the vendor to cooperate with Owner, including duties to notify breach victims if requested. The Organization should also compel vendors to provide notification to any known vulnerabilities that the vendors are, or become aware of.

BEST PRACTICE GUIDELINES

5. **Acts or Omissions**
   Language should explicitly indicate that any acts or omissions of vendors' sub-contractors are deemed to be the same as acts or omissions as those of the Vendor. This obliges the Vendor to more closely scrutinize their supply chain partners.

6. **Indemnification**
   The Organization should have language to require the Vendor to defend, indemnify and hold harmless Owner and its Affiliates against any and all claims, judgments, losses, payments, costs (including costs related to the provision of notices to customers and/or consumers, and ongoing monitoring services), expenses (including but not limited to expenses related to investigation and reasonable attorneys' fees), damages, settlements, liabilities, fines and penalties of the Organization arising from or relating to a Security Breach and or Unauthorized Disclosure of Owner Data.

7. **Vendor Personnel Security**
   The Real Estate Organization should compel Vendors to complete appropriate background checks upon their employees and to have a process to remove access to your systems when access is no longer required. The Vendor's employees should be trained on the organizations' security requirements. Cleartext, generic or group user credentials should be explicitly forbidden. Ideally, time bounded access credentials and logging should be used to provide and monitor access.

8. **Test Environment vs Production Environments**
   The Real Estate Organization should mandate stress testing of the Vendors' system in a Test (or Development) environment reflective of the organization's environment prior to placing it into the Production environment. Should the system be required to interact with other Owner systems, system integrations should be stress tested as well.

9. **Certification and Right to Audit**
   The Real Estate Organization should require Vendors to provide Security Certifications (i.e. SOC II, WebTrust, ISO 27001, etc..) and /or independent assessment of the Security Controls reflective of the risk environment and advise Vendors of the Owners' right to audit Vendors Security Controls and environment.

10. **Business Continuity Plans/Disaster Recovery Plans and Right to Review**
    The Vendor should provide the Real Estate Organization their overarching Business Continuity and Disaster Recovery Plans to ensure an understanding of how both entities will interact in the event of a short, mid and long term system failure. These plans should address Recovery Time and Recovery Point Objectives, and specific Service Level Agreements between both parties to ensure adequate compensation related to those SLAs.

11. **Penetration Testing**
    The vendor should allow the Real Estate Organization to conduct penetration testing, or alternatively that the Vendor provides third party verification. The Vendor should be obligated to remediate any negative findings within a specific timeframe.

12. **Insurance**
    The Vendor should be required to maintain:
    (i) Commercial General Liability Insurance
    (ii) Professional Liability Insurance
    (iii) Privacy/Network Security (Cyber) Liability Insurance
    with limits *in alignment with the Organization's requirements per occurrence.*

BEST PRACTICE GUIDELINES

13. **Location of Servers**
    Depending upon Data Protection legislation, the Real Estate Organization may wish to consider stipulating the geographic location of which the Vendor servers and data, as well as the backup and Disaster Recovery sites.

14. **Intellectual Property**
    Language should be inserted to ensure that the Vendor agrees that any part or parcel of the Services provided do not infringe upon any patent, copyright, trademark, trade secret, license or any other proprietary right of any third party.

15. **Change Management Process**
    The Real Estate Organization should stipulate that full system documentation, training, and a mutually agreed upon Change Management Process is implemented.

16. **Absence of Surreptitious Code, Malware or Backdoors**
    Contract language should include Vendor certification that the Services shall contain no harmful surreptitious code, including code designed to modify, delete, damage, deactivate, disable, harm or otherwise impede in any manner the operation of the Services or any other associated software, firmware, hardware, computer system or network (e.g., a Trojan horse, worm, backdoor, Remote Access Tools, etc.).