October 17, 2016

American Bar Association (ABA)
Cybersecurity Legal Task Force

Vendor Contracting Project: Cybersecurity Checklist[1]

Introduction

The objective of this Cybersecurity Checklist is to assist procuring organizations, vendors, and their respective counsel to address information security requirements in their transactions. The Checklist frames the issues parties should consider consistent with common principles for managing cybersecurity risk. The Checklist contemplates transactions from due diligence and vendor selection through contracting and vendor management. It suggests that cybersecurity provisions are not "one-size-fits-all," but should instead be informed by parties' assessment of risk and strategies to mitigate risk.

The ABA Cybersecurity Legal Task Force recognizes that cybersecurity is a dynamic subject, and we expect practitioners will modify and supplement the Checklist to reflect the particular regulatory requirements and business needs of their clients. We welcome your feedback and suggestions regarding the Checklist. Please send your feedback to the Task Force staff: Holly McMahon at Holly.McMahon@americanbar.org or Kelly Russo at Kelly.Russo@americanbar.org.

For convenience, the Checklist uses the term "**vendor**" to refer broadly to any third-party supplier of goods or services and the term "**purchaser**" to refer broadly to the party receiving the goods or services. The term "**agreement**" is used in the Checklist to refer to a product purchase agreement, license agreement, service agreement, or other agreement however styled to reflect the nature of the arrangement between the vendor and purchaser.

Cybersecurity Strategy – Understanding the Landscape of the Transaction

An organization's information security activities should begin before it undertakes transactions as vendor or purchaser. All organizations should establish and maintain a documented strategy for identifying and managing their respective cybersecurity risks. An organization's cybersecurity strategy should be informed by laws and regulations – federal, state, local, and international (at national, regional, provincial, and local levels) – to which the organization is subject, applicable industry standards, and business and operational requirements, including the organization's assessment of its own tolerance for risk.[2] Transactions that

[1] The Checklist was prepared by ABA members Cheryl M. Burtzel (*Austin, Texas)*, Candace M. Jones (*New York, New York)*, Lisa R. Lifshitz (*Toronto, Ontario, Canada*), and Lucy L. Thomson (*Washington, D.C.*) with valuable feedback from members of the ABA Cybersecurity Legal Task Force and the sections of Business Law and Science & Technology Law. The Checklist is the work of these individuals in their personal capacity and does not represent the policies, views, or positions of their respective employers or clients on these issues.

[2] There are many sources of law and guidance that may inform an organization's cybersecurity strategy. A number of industry-specific laws include security and privacy requirements, such as the Gramm-Leach-Bliley Act (financial services), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) (healthcare). U.S. federal regulators have issued guidance on managing outsourcing or third party risk. (See Appendix A for a partial list of those applicable to the financial services industry, for example.). Guidance also has been issued for healthcare, education, and utility industries. States have enacted laws that require organizations doing business in the state to take reasonable

introduce third parties into an organization's business operations, whether as vendor or customer, should be accounted for in the organization's business strategy. Conversely, transaction terms should account for the organization's cybersecurity strategy.

From the purchaser's perspective, vendor selection should also be informed by the purchaser's specific requirements and expectations regarding the information and information systems relevant to the vendor relationship. These requirements should anticipate controls the purchaser will implement and maintain as part of its overall information security plan for the business activity. The purchaser should have an informed and realistic view of its own environment and business needs so that it can reasonably assess the impacts (small or significant) of introducing a vendor relationship and make appropriate business judgments consistent with the purchaser's risk tolerance as well as applicable regulatory and legal requirements. Depending on the nature of the goods or service and the interconnectedness of the vendor and the purchaser, new vendors may introduce or increase information security risk, mitigate security risk, or both. Among other things, the purchaser should clearly understand the service delivery model and approach proposed by the vendor, including the vendor's proposed use of subcontractors and suppliers who may have access to or impact the purchaser's systems and data.

From the vendor's perspective, the vendor must understand how a purchaser's requirements could affect the vendor's operations. For example, supplying products or services to a purchaser in a regulated industry such as financial services or healthcare may impose requirements not addressed in the vendor's current procedures, systems, or compliance processes.

In most organizations, understanding the landscape into which a new vendor/purchaser will be introduced or new product or service will be added is a cross-functional exercise involving the people in the organization who understand the business objectives, the business process – particularly the participants and information involved – the information systems, and the organization's risk tolerance. While transaction planning will be driven by individuals responsible for the business activities to be supported by the product or service to be purchased/supplied, transaction planning should also leverage individuals tasked by the organization with responsibility for implementing, managing, and overseeing the effectiveness of its cybersecurity strategy. Organizations with established written cybersecurity governance frameworks should be better equipped to plan for and implement new or changed vendor-purchaser relationships in the ordinary course of business.

Risk Assessment – Cybersecurity Considerations for the Transaction

Organizational risk comprises many types of risk, *e.g.*, management, investment, financial, legal, safety, logistics, supply chain, and security risk. Similarly, security risk has multiple dimensions. The Checklist focuses on one aspect of cybersecurity risk, namely vendor relationships. Analyzing interconnections with and dependencies on third parties is an element of cybersecurity risk assessment and management.

---

measures to protect and secure data in electronic form containing personal information. Most U.S. states (and some Canadian provinces) have breach notification laws triggered by loss of personally identifiable information or other sensitive information. Organizations with global business operations must comply with applicable country-specific laws and may be subject to rules of intergovernmental organizations, *e.g.*, European Union, Canada, the Association of Southeast Asian Nations, Asia-Pacific Economic Cooperation, and others. Additional guidance can be expected over time.

Risk assessments should identify functions, activities, products, and services and their relative importance to the organization.[3] Organizations should also evaluate the inherent cybersecurity risk presented by the people, processes, technology, and data that support the identified function, activity, product, or service and assess the existence and effectiveness of controls to protect against the identified risk. Thus, risk assessments can provide the basis for the selection of appropriate controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level.

In the vendor context, risk assessments should inform the underlying decision to outsource any function or activity, as well as the specific requirements for a product to be supplied or service to be performed. Risk assessments and controls should also be referenced in the vendor due diligence and selection process to identify gaps or deficiencies that will need to be addressed by the parties to mitigate risk. At the end of the day, it is in the interest of both vendor and purchaser to identify and mitigate cybersecurity risk.

The parties' cybersecurity strategies and risk assessments will be key to establishing a solid foundation for the vendor selection process. At the vendor selection stage, the prospective purchaser should consider the following:

1. The nature of the goods or services to be purchased/supplied and identify the information and assets relevant to the vendor engagement. What information will the vendor receive from the purchaser, collect on the purchaser's behalf, process, transmit to third parties, and/or store? How sensitive are the data? Do the data include personally identifiable information ("PII"), financial information, protected health information, proprietary information and trade secrets? The inventory of relevant data should include data stored on networks, in third-party data centers, on mobile devices (laptops, portable storage, smartphones), in the cloud, on back-up devices, and in industrial control systems.

2. What is the purchaser's risk profile for the product or service needed? That is, what: (a) information will be processed or stored; (b) access to systems or internal operations will be given to a vendor; and (c) customer-facing activities will be impacted? Does the product or service support critical operations? Will the vendor interact directly with the purchaser's customers or clients or have access to systems or portals through which customers or clients interact with the purchaser?

3. What access will the vendor or purchaser need to have to the other party's information or information systems? What controls does the party whose systems will be accessed have in place to manage such third-party access to its information or information systems? Are the existing controls likely to be appropriate for managing the party to be given access?

---

[3] Risk assessments can inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (*i.e.*, harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur.

There are many risk assessment frameworks and guidance documents available, including some that are industry-focused. For example, see the *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology (NIST), February 12, 2014, and other NIST publications and guidance cited in the Framework.

4. What are the applicable legal/regulatory requirements for the product or service in the context of the purchaser's business? Does the vendor have experience supplying the relevant product or service to others in the purchaser's industry? Legal requirements from multiple jurisdictions (federal, state, local, and international) and regulatory disciplines (*e.g.*, financial, healthcare, consumer) may apply.

5. What are the applicable commercial requirements, including obligations to the purchaser's customers or business partners, to protect information the purchaser processes or stores for those third parties?

6. What interdependencies will be relevant to effective management of the vendor? Purchasers need to consider the web of customers, vendors, and affiliates who may have a role in delivering or using the product or service or whose information may be provided to the vendor.

7. Will the vendor be providing the goods and services exclusively or will it be working with third parties, including subcontractors? Purchasers will require a good understanding of the prospective vendor's subcontractors and downstream partners as the use of multiple subcontractors and third-party providers will further impact and complicate vendor due diligence and cybersecurity management.

8. What power or influence do the parties exercise in the relevant marketplace? If the negotiating power of either party is outsized relative to the other, responsibility and risk may not be allocated in a way that aligns rationally with the role each party will have in the transaction or the ongoing supply of the product or service. In any case, a party that does not get what it believes is necessary to address its information security expectations will have to determine how, if at all, it can implement controls that mitigate the deficiencies it perceives in the relationship (compensating controls) or it may have to consider other options, including other vendors or other ways of satisfying the business need or otherwise mitigating risk as well as the possibility of covering some risk through the purchase of cyberliability insurance, for example.

Vendor Due Diligence

As part of the vendor selection process, purchasers should evaluate the capacity of prospective vendors to follow appropriate information security practices in producing and delivering goods and performing services. The purchaser's assessment of its own business and risk management objectives should inform the purchaser's due diligence activities.[4]

Vendors also learn through the due diligence process about the prospective customer's cybersecurity requirements and expectations. In many cases, vendors have more experience and a deeper understanding of relevant systems and cybersecurity threat landscape than their customers. Vendors may seek through their own due diligence information about the purchaser and third parties with which the purchaser expects the vendor to interact. Cybersecurity is not a

[4] Key elements of NIST's Special Publication 800-171 (June 2015), *Protecting Controlled Unclassified Information in Nonfederal Information Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, are summarized in Appendix B.

zero-sum proposition; both parties have an interest in identifying appropriate controls and placing responsibility where risk can best be mitigated.

The parties should be assisted by qualified information security personnel during due diligence and throughout the vendor relationship, as appropriate. To the extent weaknesses are identified during the due diligence phase, the parties' business people (informed by their information security experts) will need to weigh the risks of those deficiencies against the benefits of the transaction and consider appropriate mitigation. This initial assessment and the plan for any agreed remediation should inform the agreement. After completing its due diligence, the purchaser may also need to reassess its risk profile to account for risk arising from the vendor relationship that the purchaser will need to manage. The parties also will need to assess risk as their respective environments change or whenever additional products or services are implemented.

Due diligence activities generally should accomplish the following:

1. Conduct a security assessment of the vendor**,** which may be a direct assessment by the purchaser or its agent, review of vendor self-assessment or third-party assessment reports, or some combination of those activities. The scope of the security assessment should be informed by the nature of the product or service, its relative importance to the purchaser, and the sensitivity of information the vendor will collect, store, process, or transmit for the purchaser. Qualified information security personnel should assist the purchaser to identify relevant areas of assessment and to evaluate the information provided by prospective vendors. At a high-level, a security assessment should consider the extent to which the vendor[5]:

   (a) has adopted appropriate security policies and procedures, including written policies as necessary to create a "culture of security," and enforces its security procedures, particularly those most likely to prevent the most common types of data breaches;

   (b) has created appropriate incident response and business continuity/disaster recovery (BC/DR) plans and tests and updates them regularly;

   (c) maintains a program to manage compliance with applicable federal, state, local, and international laws, including laws prohibiting unfair or deceptive practices, data breach, data disposal, privacy and confidentiality of personal information and other protected records, as well as laws or regulations that restrict use of certain information without appropriate consent; and

   (d) addresses information security in a manner that enables the purchaser to demonstrate the purchaser's compliance with applicable laws and regulations, taking into account controls the purchaser inherits from the vendor.

2. Assess the vendor's program to maintain its IT infrastructure and operations consistent with cybersecurity objectives, including those of the purchaser. To what extent does the vendor implement and use software and hardware with security and privacy built into the

[5] A complete security assessment guide is outside the scope of the Checklist. Parties should consult employees and advisors with appropriate security expertise.

design of the product? To what extent does the vendor assess the secure development practices of third parties supplying custom and critical applications? How does the vendor monitor its systems for known vulnerabilities and respond to newly-reported vulnerabilities? Does the vendor have a procedure to monitor vulnerabilities identified in authoritative sources and other threat intelligence? Does the organization adhere to practices of scanning software for vulnerabilities before it is installed and for avoiding implementation and use of software and hardware for purposes for which they were not designed? Where and when does the vendor encrypt data in its possession or control? Does it send any data over unencrypted channels?

3. What incidents/breaches and vulnerabilities has the vendor identified in the vendor's systems (including systems provided to it or hosted by the vendor's suppliers and service providers) and what are its plans for remediation? The information requested from the vendor should be reasonable under the circumstances and tailored to the type of product or service the vendor will provide. For example, the parties should anticipate closer scrutiny when the vendor will have access to sensitive customer data or PII, provide a product that affects the security of an organization broadly, or will be a key part of the purchaser's critical infrastructure. If a vendor is not willing to provide the requested information, consider what assurances the purchaser should request about how the vendor manages vulnerabilities and incidents, generally? In this context, the parties may also have an interest in knowing about their counterparties' experience in matters involving law enforcement or regulatory authorities as well as communication plans and infrastructure in place to communicate if/when an incident occurs.

Contract Provisions – Setting Expectations, Mitigating Risk, and Allocating Liability

The material covered in this list is intended to highlight provisions that should reflect information security considerations even though the substance of the provisions is not necessarily limited to information security. The Checklist does not cover contract terms not likely to reflect information security considerations (*e.g.*, payment terms). The agreement between the purchaser and selected vendor should contemplate the entire vendor lifecycle, including performance monitoring, effective communication (including information about cyber threats and incidents), performance obligations of the parties, and winding up and offboarding activities at the end of the relationship (including the secure return/erasure of the purchaser's data).

Contract provisions, including elements that address cybersecurity, are not one-size-fits all. As reflected in the commentary above about cybersecurity strategy and risk assessment, contract provisions should be appropriate for the transaction and, of course, reflect the mutual understanding of the parties. Because all parties to a transaction have a shared interest in identifying and mitigating cybersecurity risk, many provisions relevant to cybersecurity necessarily define processes and allocate responsibility.

1. **Definitions**. Define key terms related to information security. For example:

   (a) Confidential information;

   (b) PII;

(c) Incident and data breach[6];

(d) Malware or similar concepts like "harmful code" which cover, in addition to viruses, other undisclosed functionality, e.g., backdoors, self-help tools, remote access; and

(e) Vulnerability[7] – consider features or functionality that by nature or design could also be vulnerabilities.

2. **Performance** – Consider how the description of a product or service to be delivered by the vendor implicates information security. Also consider responsibilities of the purchaser, whether stated explicitly or imposed implicitly by the limitations of the vendor's product or service.

(a) What is the nature of the product or service to be delivered or performed and for whom – the purchaser, purchaser's affiliates, the purchaser's customers?

(b) Who will produce the product or perform the service and, thereby, have access to the purchaser's information or systems? Anyone other than the vendor, *e.g.*, affiliates, subcontractors, downstream vendors/suppliers? How far down or out in the vendor ecosystem a purchaser pursues information security and assurances as to performance will depend on the purchaser's judgment and applicable legal requirements.

Note: The parties should consider what steps will be taken to monitor the role of third parties. The purchaser might review the vendor's vendor management program or insist on direct access to the downstream vendor for review and monitoring as well as being identified as a third-party beneficiary of subcontracts. The approach taken should be commensurate with the significance of the role of the third party. As a practical matter, purchasers often rely on vendors to manage their third-party suppliers – at the risk of liability to the purchaser – because other arrangements are too disruptive, inefficient, and resource-intensive.

(c) How will the contracting parties interact and share and manage information? Will the vendor have direct access to the purchaser's systems for any reason, including maintenance and support?

(d) Does the vendor need, or will it be given permission to use, the purchaser's information, technology, and intellectual property (IP) (such as the purchaser's name, logo, trademarks, and copyrighted material)? If yes, will the vendor be authorized to

[6] Consider the distinction between "incident" and "breach" illustrated by HIPAA definitions. HIPAA regulations define "security incidents" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 CFR § 164.304 The breach notification rule in HITECH defines breach as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information . . . ." (See the definition of "breach" at 45 CFR § 164.402.) "Incident" is broader in that it covers attempts as well as actual compromise.

[7] The NIST *Glossary of Key Information Security Terms* (Rev. 2 May 2013) presents a few definitions of "vulnerability," including these: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" and "A weakness in a system, application, or network that is subject to exploitation or misuse." (Internal citations omitted.)

allow its affiliates, subcontractors, and suppliers to have access to the purchaser's information, technology, or IP and subject to what conditions? What legal assurance will the purchaser have that the vendor manages any downstream sharing (including to third-party subcontractors, affiliates, and other providers) effectively?

(e) What records, data, information, and analytics will the vendor create during the term of the contract and who will own them? Who will have access to those records? Does the vendor intend to make any secondary usage of such data, information, or analytics? Where will those records be located? On what terms and through what channels will the purchaser or its representatives have access to those records?

Note: Agreement about "ownership" of records created in the course of performing services can be elusive. It is often more productive to focus on how the data will be used and stored. A more comprehensive discussion of data ownership is outside the scope of the Checklist.

(f) Where will products be produced or services performed? Location considerations may include continuity and infrastructure risk, political risk, and security risk. Beyond the vendor, consider subcontractors and downstream suppliers, particularly those critical to products and services supplied by vendor to purchaser. If the purchaser operates subject to regulatory restrictions on foreign service providers, for example, those restrictions should be addressed with respect to the vendor's subcontractors and suppliers.

3. **Representations and Warranties**. Depending on the circumstances, particularly bargaining leverage, a purchaser may need to adapt the representations and warranties listed below and may not be successful in obtaining representations and warranties in the form the purchaser would prefer to have.

(a) *No recent security incidents/breaches not disclosed to the purchaser*.

Note: This representation implies that the vendor has provided relevant information during the vendor selection and due diligence process. Use of "incident" or "breach" in this context will be informed by the definitions of those terms and may be qualified with an appropriate materiality standard.

(b) *No claims threatened or pending, or events or circumstances known to the vendor likely to give rise to claims as a result of any security incident or vulnerability*.

(c) *No regulatory actions threatened or pending, or events or circumstances (noncompliance) known to the vendor likely to give rise to regulatory action as a result of any security incident or vulnerability*.

(d) *No processing, storage, or transmission of purchaser's information by third-parties not disclosed to purchaser.*

Alternative example: *Vendor's information storage and handling procedures comply with [insert relevant sector-specific laws, e.g., Gramm-Leach-Bliley Act section*

501(b) if handling information for financial institutions and HIPAA/HITECH if handling personal health information], as applicable.

Note: This representation will be complicated if the vendor uses cloud services for processing or storage. The vendor will have to consider the operations of the cloud provider.

(e) *Vendor has all licenses and certifications required by applicable law to provide the product/ perform the service.*

In this regard, consider particular licenses and/or certifications that may be required for handling the purchaser's information, if any.

(f) *Vendor has all rights necessary to provide the product, software, and data and other information, and perform the service as contemplated by the contract. If vendor licenses any software, data, or other content necessary to perform a service for purchaser, vendor's licenses authorize vendor to use the licensed material to perform the service for third parties*.

Note: This representation may be more directly relevant to continuity of service than to cybersecurity. However, information about the maturity of the vendor's business procedures to manage its products and third-party content may be indicative of the vendor's maturity in other aspects of its business, including cybersecurity.

(g) *Vendor has an information security program in place as required by the agreement [cross-reference the relevant section]*.

Alternative example: *Vendor has identified no deficiencies in its information security program when measured against [contract requirements – appropriate internal cross-reference] that have not been disclosed to the purchaser and accepted or are the subject of an appropriate plan of action and milestones to remediate in a manner acceptable to purchaser.*

Note: If the purchaser identifies deficiencies in its due diligence, the purchaser should account for the deficiencies either by acceptance (which may entail additional controls established by the purchaser) or with an undertaking by the vendor to remediate against an agreed plan of action and milestones. The latter should be documented in the parties' agreement. The parties should be mindful of limiting information in the text of the agreement about deficiencies and remediation. For example, referencing a plan of action and milestones that bears indicia of acceptance, but not attaching or restating the plan directly in the agreement can help limit specific vulnerability details to those who need to know them.

(h) *Vendor employs personnel qualified to maintain the information security program*

Note: If vendor outsources information security activities, the purchaser should be provided notice if the vendor changes providers and have the right to receive information validating that the information security program is the same or better.

(i) *Vendor handles information collected from purchaser (or purchaser's customers) consistent with the practices for information handling described in policies and procedures, including its privacy policy and other terms posted on its website or otherwise published to users.*

4. **Confidentiality**

(a) *Mutual*. Do both parties have confidential information of the other? Do all provisions apply equally and reasonably to both parties?

(b) *Scope.* Define confidential information (definitions section) in the possession or control of each party, where "control" encompasses information entrusted by the receiving party to any third party. The parties also should address scope of confidentiality applicable to data generated by the performance of the agreement.

(c) *PII.* Will the vendor collect, store, process, or transmit PII? From what jurisdiction(s) does the PII originate and where will it be stored? For an example of a confidentiality provision written from the perspective of a Canadian purchaser, see Appendix C.

(d) *Permitted uses of confidential information.* Generally, confidential information should be used only as necessary to perform the service, furnish the product, and administer the agreement. If other uses are permitted, under what conditions and how will those other uses be monitored? The parties also should address the use of data created by the performance of the agreement.

(e) *Storage & Communication*. Restrictions on location, notice of storage in any location not previously disclosed; *encryption* of data-at-rest and in-flight/transit.

(f) *Sharing with affiliates and downstream vendors/subcontractors*. Under what circumstances and subject to what conditions? How does the vendor track and manage information provided to its subcontractors and service providers and flow-down requirements in customer contracts and other applicable law? How will the vendor provide assurance of compliance by downstream recipients? The same questions apply with respect to vendor confidential information given to the purchaser.

(g) *Customer-supplied information and "record information," i.e.*, information accumulated about customers or as a byproduct of the customer relationship (profile) – see note above about ownership of record information.

(h) *Return/destruction obligation* at the end of contract term and at other times at the disclosing party's request. No vendor should be allowed to retain PII forever, especially after the contract has been terminated (and in some jurisdictions the perpetual retention of PII after it is no longer required is in fact a violation of applicable privacy laws). *Note*: Requests made other than at the end of the term or following a breach should be conditioned so that the disclosing party cannot use the provision to impair the performance of the recipient or deprive the recipient of the benefit of the contract.

(i) *Exceptions to return* – Will the disclosing party agree to exceptions, such as for information stored in secure back-up in a manner that makes destruction of specific purchaser information impractical/ commercially unreasonable? Many laws and regulations require entities to destroy, dispose of, or otherwise make personal information and business records unreadable or undecipherable.

(j) *Incident management*. Effective incident management supports the ability of the parties to respond and recover. Both parties have a stake in containing incidents and mitigating adverse impact. The parties may be required by law or regulation – if not by the circumstances directly – to coordinate response and recovery activities. The incident management provisions should address:

i. The definition of "incident."

ii. Notices to affected persons and law enforcement – timing, content, method of delivery.

iii. Delays attributed to law enforcement activity – should delay be permitted?

iv. Copies of any notice (or notices containing the same information) vendor is required to give to its customers, affected persons, regulators or other authorities in connection with any incident, unless prohibited by law from doing so.

v. Vendor's procedures/infrastructure for tracking notice requirements and implementing notices when required, including notices to purchaser and notices required by law. Consider notices required by laws to which vendor is subject, as well as notices required by laws to which purchaser is subject. More generally, understanding vendor's systems (people, process, technology) for giving notice should factor into the purchaser's assessment of a vendor's ability to comply with contractual notice requirements.

vi. Access to information about incidents and to compromised systems or images to assess the impact of an incident and mitigate adverse effects. Consider obligations that may be imposed on both parties by applicable law or regulatory requirements.

vii. Remediation – access to information about root cause and observed impacts to aid response and recovery.

viii. Costs – allocate liability for direct costs of the incident, such as breach notification when personal information is compromised, as well as other costs that result.

ix. Duration of confidentiality obligation – indefinite (as long as a party is in possession or control of other party's confidential information). If a confidentiality obligation is not indefinite, the disclosing party must take steps to confirm that the recipient returns or destroys the information before the confidentiality obligation expires. Failure to do so would be equivalent to

permitting unrestricted use and disclosure at the end of the confidentiality period.

5. **Security program**. Generally, the purchaser should seek the vendor's commitment to establish and maintain a comprehensive security program to maintain the confidentiality, integrity, and availability of information and systems commensurate with the consequences and risk of loss, misuse, and unauthorized access to or modification of information.

   Employees with responsibility for cybersecurity and information security advisors who support them should assist the parties to identify appropriate elements of a security program commensurate with the cybersecurity risks. Consider, for example, the following specific subject matter for security program obligations:

   (a) *Physical controls*.

   (b) *Administrative, management, technical, and logical controls.*

   (c) *Vulnerability management* – monitoring for threats, including malware, viruses, intrusions, *etc*., and response and remediation procedures.

   (d) *Software management* – program for assessing risk associated with applications, whether developed by vendor or licensed from a third-party. Does vendor follow secure development practices for internally-developed software? Does vendor assess secure development practices of third parties supplying custom and critical applications?

   (e) *Infrastructure maintenance* – regular patching and other maintenance activities that protect systems and keep the infrastructure operating at committed service levels. Are maintenance activities prioritized to consider information security risk as well as operational risk/performance?

   (f) *Personnel* – qualifications of employees with cybersecurity responsibilities and access to purchaser's systems or data; policies and training; insider threat program, including monitoring and enforcement, background investigations, segregation of duties, least permissions/privilege protocols for access to systems and information.

   (g) *Compliance with specific requirements of applicable law or regulatory requirements*, *e.g*., HIPAA/HITECH if handling personal health information, GLBA 501(b) if handling information for financial institutions, and international laws and regulations as applicable for non-U.S. operations and non-U.S. customers.

   (h) *Threat assessment/intelligence monitoring* – vendor procedures to monitor dynamic threat environment.

   Note: The purchaser should also consider its own activity to monitor third-party intelligence about vendor products and services used by purchaser.

   (i) *Change management* – change management procedures for relevant vendor systems; notification of changes that could affect security assessments.

6. **Monitoring/Assessment of Vendor Performance.** Monitoring and assessment provisions should be included in the agreement and require appropriate remediation activities and mechanisms to exit the relationship if issues identified cannot be adequately addressed.

   (a) *Performance* relative to agreed service level commitments, key performance and risk indicators.

   (b) *Vendor entitlements to purchaser information and systems* to align with purchaser's current risk tolerance, *i.e.*, purchaser may remove vendor entitlements as necessary to maintain purchaser security – even if vendor performance is impaired. The contract should address notice and adjustment to changed conditions for access to information and systems. If the purchaser has access to vendor systems, reciprocal provisions should also be considered.

   (c) *Audit*, whether purchaser audit, vendor self-assessment and certification, or third-party audit, of internal controls, reporting, contract performance, security/technical, and the like. Security audits may occur periodically and be event-driven. Audit provisions may provide that the results of third-party audits be made available to purchaser (*e.g.*, upon request or according to an agreed upon schedule), together with evidence of remediation of risks identified and explanation of any risks accepted (that is, disclosed to purchaser and not remediated). Consider the level of audit detail accessible to purchaser (*e.g.*, conclusions versus entire report), as well as expectations regarding severity of risks that must be remediated versus risks the vendor may accept.

   (d) *Financial review* – relevant to: (1) assess the capability of the vendor to make investments in operations that enable continuous monitoring and on-going attention to the changing environment/threat landscape; (2) evaluate risk of loss of service if vendor fails; and (3) evaluate risk of loss of information if vendor fails and purchaser is unable to recover information from vendor or its downstream service providers.

   (e) *Remediation* – process to develop plan of action/mitigation with opportunity for purchaser to review and determine adequacy or take steps to suspend or terminate some or all vendor products/services.

   (f) *Vendor personnel background investigation* – conducted by purchaser or conducted by vendor. Consider legal constraints on individual background investigations.

   (g) *Access to vendor information, systems, and operations for audit/assessment by purchaser's regulators*. If the purchaser is a regulated entity, are the vendor's activities subject to regulatory examination or oversight by the purchaser's regulator, including access to work papers, drafts, and other materials?

7. **Risk Event Reporting** – events beyond breach/security incidents, *e.g.*, loss of material downstream supplier, political risk or labor disputes in a location where key services are performed, and IP infringement claims that could enjoin use of key technology.

8. **Remedies**. Remedies should be appropriate for the nature of the failed performance and actionable. For example, infrastructure to provide a timely response, including escalation procedures, commensurate with the severity of a defect or vulnerability may be as important to mitigate loss than a damages provision.

   (a) *Elements of loss that will be compensable as damages*. For example, is the purchaser responsible for its own expenses to investigate and mitigate vulnerabilities related to the vendor's product or service, including costs for unscheduled upgrades, or are those costs compensable as damages?

   (b) *Liquidated damages*. Are liquidated damages an appropriate or effective remedy for some elements of loss arising from cybersecurity incidents?

   (c) *Specific performance* – is specific performance of cybersecurity covenants an available/enforceable remedy? Can contracting parties agree to specific enforcement as a remedy? Would such an agreement be enforceable?

   (d) *Limitations and disclaimers* – Consider incidental and consequential damage disclaimers as they relate to security breaches. What costs arising from response and recovery are direct damages and what costs are incidental/indirect?

9. **Termination**

   (a) *Default* – What acts, omissions, or conditions give either party the right to terminate? Should breach of certain cybersecurity obligations be defined as "material" for purposes of establishing the right to terminate? Will termination be an effective remedy – as a practical matter?

   (b) *Is either party permitted to terminate under circumstances other than default (*e.g., *upon reasonable notice and without penalty)*:

      i. In the event a regulator formally directs the purchaser to terminate the relationship or regulatory or legal requirements change in such a way that they are not satisfied by the vendor arrangement?

      ii. In the event the vendor is unable to provide an adequate response to a cyber threat?

      iii. In the event the purchaser and vendor disagree about the significance of a vulnerability or the plan to remediate?

      iv. For convenience – which could enable exit when the purchaser does not believe it has received adequate assurance of continuing performance of cybersecurity obligations.

   (c) *Transition Plan* – services to facilitate orderly winding up and transfer of data and/or services back to the purchaser or to an alternate vendor. Consider any hardware, third-party software, data, record information, space leases, IP and other assets or support that will be required for continued operation and should be assigned or transferred at the expiration or termination.

(d) *Offboarding/Turnover obligations* – verification/certification of return or destruction of purchaser data and information, return/deactivation of credentials controlled by vendor, cooperation with orderly removal of vendor personnel access to purchaser (physical and logical access), transition assistance. Ensure that the agreement requires the vendor to oversee its affiliates' and subcontractors' compliance with the above.

10. **Insurance** – consider cyber risk insurance coverage from both the vendor and the purchaser perspectives. Insurance is not, however, a substitute for reasonable due diligence and diligent contract and performance management.

11. **Indemnification**

(a) *General*

(b) *Loss of information* – costs associated with breach notification (including regulators, individuals and other organizations), investigation, remediation (*e.g.*, credit reporting, specific actions required by applicable regulators/governmental authorities, and contractual obligations such as payment processor contracts) and litigation expenses.

(c) *Intellectual property*

Note: Be aware of disclaimers of liability for third-party materials. For example, most open source licenses disclaim liability associated with any use of the licensed material. If the vendor also disclaims liability for third-party material (software components or other content), the purchaser will bear the risk of loss associated with the component.

(d) *Limitation of liability* – If the agreement will include limitations of liability, consider carve-outs or separate caps for indemnification of third-party claims – particularly claims based on information loss, costs associated with security and data breaches, and IP infringement – as well as costs to remediate vulnerabilities and incidents.

12. **Business Continuity/Resiliency** – Consider what priority the purchaser will be given by the vendor in a contingency situation that impairs the vendor's performance. Knowing whether or not the purchaser is a critical customer should inform the purchaser's business continuity/resiliency planning. Also consider prioritizing the products supplied and services performed by the vendor so that there are established expectations about how limited resources should be directed. The agreement may point to an agreed upon contingency plan and provide a process for periodic review and update.

(a) *Disaster recovery* – retention and back-up procedures, ability and time to failover to redundant systems, and security of back-up facilities.

(b) *Ownership/license of material to maintain operations/support* – Do the parties have the rights each needs to shift performance (internally or to a third party) in a contingency situation?

(c) *Identification of key personnel*, including personnel with *security* roles, and training for contingency situations affecting the purchaser? Does each party have direct access to key personnel in the other's organization? Under what circumstances? Is there a mechanism to validate/update contacts periodically?

(d) *Purchaser access to vendor's continuity plan and periodic testing results*. Should purchaser participate in vendor testing exercises?

(e) *Vendor participation in customer continuity and/or incident planning*. Should purchaser have the right to require vendor personnel to participate in purchaser's continuity or incident planning exercises? Under what circumstances?

(f) *Communication between purchaser and vendor* during a contingency event. Include a mechanism to validate/update communication plans periodically.

(g) *Force Majeure* - Draft to maintain performance consistent with continuity/resiliency obligations.

13. **Miscellaneous**

(a) *Notices* – Information security provisions often include notice requirements. Reconcile the notice provision with the expectation for prompt notice of incidents, vulnerabilities, *etc*. For example, a requirement to send notice by overnight delivery the next business day is not generally consistent with the expectation for timely notice of a cybersecurity incident. Also consider differing notice requirements under various applicable laws such as privacy laws where notice requirements may vary depending on the nature/sensitivity of the PII involved and international laws.

(b) *Assignment and change of control* – Consider conditions on assignment or change of control that enable reviews of operations and systems if performance is moved to a different entity.

(c) *Subcontracting* – Subcontractors may be affiliated or nonaffiliated entities and individuals (including temporary workers). If subcontracting is permitted, subject to what conditions (for example, jurisdictional/geographical limitations)? Also consider downstream vendors that provide infrastructure or perform services for the vendor not exclusive to the purchaser's contract, *e.g.*, third-party data storage providers. The parties should consider how entities are interconnected and how information can flow – intentionally or inadvertently – among them. How will those relationships be monitored? Can the purchaser terminate the contract without penalty or obtain some other remedy if the subcontracting arrangements do not comply with the terms of the contract?

(d) *Survival* – Consider confidentiality and security in relation to information retention/storage.

(e) *Dispute resolution* – Consider agreed escalation procedures that include knowledgeable representatives from both sides (*e.g.*, information security talking to

information security), to determine if parties agree on relevant facts and assessments of technical issues and risk.

14. **Software**

(a) *Open source components* – inventory, monitoring/remediation of vulnerabilities, indemnification.

(b) *Third-party components* – Same as open source.

(c) *Self-help remedies* – If not prohibited altogether, then mechanisms for self-help must be disclosed, should not be exercised without notice, and should only be exercised to prevent harm to the purchaser and/or other customer infrastructure.

(d) *Vulnerability reporting* – If the vendor supplies software, what obligation does it have to report and address vulnerabilities in the software? Consider: Scope, *e.g.*, cover all third-party components, including open source? Timing for reporting – when a vulnerability is discovered together with ongoing updates until remediated? Content – describe the vulnerability and any observed adverse effects, including nature of losses or impairment of performance? Release notes or other notice indicating that an update or patch includes changes to address vulnerabilities or enhance security.

Note: Vendors may refuse to take on obligations to give individual customers notice of vulnerabilities because they do not have systems (people, processes, and tools) in place to manage such reporting requirements. Understanding whether and how the vendor uses (or could use) its customer communications infrastructure to give notice of cyber risks may provide a path to an acceptable approach.

(e) *Threat intelligence coverage* – Vendor should identify any third-party (a) to which it regularly reports vulnerabilities, including threat monitoring services and information sharing organizations, and (b) that monitors its products; the disclosure should be updated periodically.

(f) *Support and maintenance* – Includes security monitoring and remediation of vulnerabilities – clear SLAs for response to vulnerabilities. Who determines severity – and what if purchaser's assessment of severity is different from the vendor?

(g) *Secure development environment and secure design practices* – Representations regarding present environment and promise to maintain; reference industry standards/best practice and any applicable regulatory requirements.

(h) *Warranties* – For example, no known vulnerabilities not disclosed to purchaser, no breaches of development environment not disclosed to purchaser; no undisclosed functionality; no infringement claims pending or threatened.

(i) *Escrow arrangements* for source code and other materials the purchaser might need to use the software during the license term notwithstanding vendor failure or impairment.

Appendix A

Federal Financial Regulator Guidance – Third Party Providers

Group of 7 ("G7"), Fundamental Elements of Cybersecurity for the Financial Sector, *available at* https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf

Federal Deposit Insurance Corporation (FDIC), Guidance For Managing Third-Party Risk, *available at* https://www.fdic.gov/news/news/financial/2008/fil08044a.html

Office of the Comptroller of the Currency, Risk Management Guidance, OCC-Bulletin-2013-29, *available at* http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Guidance on Managing Outsourcing Risk, Board of Governors, Federal Reserve System, December 5, 2013, *available at* http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

CFPB Bulletin 2012-13, Service Providers (April 13, 2012), *available at* http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf

FFIEC Guidance on IT Service Providers (October 2012), *available at* thandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf

Securities and Exchange Commission (SEC), Guidance Update No. 2015-02, Cybersecurity Guidance (April 2015), *available at* https://www.sec.gov/investment/im-guidance-2015-02.pdf

Appendix B

In various guidance documents, the National Institute of Standards and Technology (NIST) has identified key areas that must be addressed in a security program. Examples include:

Access Control

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Limit information system access to the types of transactions and functions that authorized users are permitted to execute

Examples: Establishing access controls and identity management protocols, including multi-factor authentication; Limits on privileged users

Awareness and Training

- Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
- Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability

- Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
- Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Configuration Management

- Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- Establish and enforce security configuration settings for information technology products employed in organizational information systems

Examples: Malicious activity scanning; Regular software patching

Identification and Authentication

- Identify information system users, processes acting on behalf of users, or devices.
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response

- Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
- Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

Maintenance

- Perform maintenance on organizational information systems.
- Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection

- Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.
- Limit access to CUI on information system media to authorized users.
- Sanitize or destroy information system media containing CUI before disposal or release for reuse.

Personnel

- Screen individuals prior to authorizing access to information systems containing CUI.
- Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Physical Protection

- Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- Protect and monitor the physical facility and support infrastructure for those information systems.

Risk Assessment

- Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.

Security Assessment

- Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

System and Communications Protection

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity

- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
- Monitor information system security alerts and advisories and take appropriate actions in response.

NIST Protecting Controlled Unclassified Information in Nonfederal Information
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Spec Pub 800-171 (June 2015), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Appendix C
Sample Provision Covering Personally Identifiable Information[8]
Canadian Law Perspective

- [Create definitions of "Applicable Privacy Laws"] – "Applicable Privacy Laws" means (i) all applicable data protection legislation, including xxxx, as same shall be amended, modified, restated or replaced from time to time; (ii) any applicable court judgments, rulings, findings, interpretation bulletins, orders, guidance documents or fact sheets issued by XXXX pertaining to the foregoing legislation; (iii) any internal Customer rules or guidelines related to data security, data integrity, privacy and the safeguarding of personally identifiable information (PII) as of the Effective Date and thereafter; and (vi) and those data protection and other laws, policies, agreements and guidelines of applicable to Customer in XXXX and elsewhere, if any; and

- "Authority" means any government authority, agency, body or department, whether federal, provincial, state or municipal, having or claiming jurisdiction over the Agreement and "Authorities" means all such authorities, agencies, bodies and departments;

- "Data Breach" means a possible or actual access, use, disclosure, copying, modification, loss or destruction of PII, which is not authorized by the terms of this Agreement or any related agreement or any other circumstance which to the knowledge of Vendor jeopardizes or may in the future jeopardize the privacy of individuals, the confidentiality or security of PII or of any system in the custody or control of the Vendor or its Subcontractors which is used to store PII, arising from a breach of Vendor's or its subcontractors' security safeguards or otherwise.

- "Inquiry": means a request for access or correction pursuant to the Applicable Privacy Laws, or an application, inquiry, challenge, complaint, review, audit, investigation, request, search or demand made in respect of PII by any third party including any Authority, with or without judicial authorization.

- "Subcontractors" means any third party retained by Vendor to provide services on behalf of or otherwise fulfill an obligation of Vendor under this Agreement, including by not limited to any Vendor Affiliate or third party subprocessor.

- Additional Obligations relating to PII
- Additional Representations Regarding PII. Vendor agrees (i) that PII is confidential and shall not be disclosed by Vendor except for the purpose of providing the Cloud Services, the Consulting Services or for the exercise of the parties' rights and obligations under the Agreement or at law, unless the owner of such PII provides express consent in writing; (ii) that PII may be disclosed only: (a) to Vendor, it Affiliates and Subcontractors for the purposes described herein unless otherwise instructed by the Customer; (b) in accordance

[8] In Canada, the actual term used under various federal and provincial private sector privacy laws is "personal information," but this term was changed in the Checklist for the convenience of the American reader. Please also note that the above would be additionally modified if personal health information was involved.

with the written requirements of an Authority to which Vendor is subject; or (c)as otherwise required by law.

- Obligations of Vendor re PII. Vendor shall maintain the security of PII in its custody or under its control in compliance with Applicable Privacy Laws, and shall protect it against such risks as unauthorized access, collection, use, modification, copying, disclosure or disposal and similar risks using all appropriate administrative, physical, technological and procedural safeguards. Notwithstanding the generality of the foregoing, Vendor represents and warrants that it shall:

    - Not process or use PII for any purpose other than as strictly required to perform the Services or any other ancillary services;
    - maintain a current inventory of all records of PII in its custody;
    - ensure that it has practices and procedures which protect the security of PII in its custody or under its control;
    - ensure that access to PII is on a need-to-know basis only;
    - ensure that the physical security of the records containing PII is protected by storing them in a secure area, restricting access to them and applying procedures for removal and copying;
    - ensure that its electronic systems containing PII are kept secure using regularly updated and patched security measures that are consistent with best practices for the protection of sensitive PII, and that the security measures used include passwords, strong firewalls, and encryption.
    - ensure that its system is encrypted at a minimum XXX bit, to be increased as appropriate to maintain consistency with reasonable business standards in respect of sensitive PII;
    - ensure remediation is done regularly as deemed necessary by current best practices;
    - ensure that each person who may have access to PII is required to sign a confidentiality and non-disclosure agreement and is made aware of their confidentiality obligations and Vendor will not will not transfer or disclose such PII to any other third party (other than its Affiliates and Subcontractors) without the prior written consent of the Customer;
    - ensure that each user of any Services that may have access to PII, including all Vendor personnel and Subcontractors, is electronically authenticated prior to obtaining access to PII using strict registration and validation processes and authentication and access controls;
    - ensure that PII cannot be viewed by unauthorized persons while it is being used for the purposes of the Services;
    - ensure that Vendor has the capability to create audit trails which record the identity of users of systems under the control of Vendor, the date and times users view, access or use PII or attempt to do so, and issues notifications to Vendor where such activity may be inconsistent with this Agreement;
    - cancel all rights of any contractor, employee or Subcontractor of Vendor to access PII immediately upon his or her departure from the team providing the Services or otherwise;

- upon request, Vendor will cooperate with the Customer in responding to any requests by authorized users to allow access to, correct, block, suppress or delete any such PII that it holds on behalf of such authorized user;
- ensure that all offices which hold PII, including home offices, are locked so that only authorized individuals have access to the PII;
- ensure that all PII held in paper form is stored in locked file/storage cabinets when not in use;
- ensure that PII remains secure when transporting, transmitting or moving such information;
- ensure that no PII is left unattended in an unsecure location;
- ensure that all PII collected, received, handled or processed by it under this Agreement, irrespective of the format in which it is contained, is protected against loss or theft, as well as unauthorized access, disclosure, copying, use or modification by security safeguards appropriate to its sensitivity, amount, distribution, format and method of storage. Such security safeguards shall comply with all Applicable Privacy Laws and shall provide at least the same or similar use of its most sensitive PII. Such security safeguards shall include, if applicable, physical measures, organizational measures (security clearances, limiting access on a "need-to-know" basis), and technological measures (such as the use of passwords and appropriate encryption);
- maintain at all times during this Agreement appropriate disaster recovery and back-up plans and ensure procedures are in place with respect to the PII in its possession. Vendor agrees that from time to time, it will review its procedures with respect to security safeguards through risk assessments, benchmarking or other means, to determine whether they are still consistent with Applicable Privacy Laws, appropriate to the risks, and consistent with best practices, and if not, agrees to revise the same as required;
- ensure that its contractual relationship with any Subcontractor requires such a party to maintain the confidentiality and security of PII, to collect, use, transfer, store, disclose, process and handle all PII it receives under such contract in compliance with Applicable Privacy Laws and restricts the use by the subcontractor, or service provider of the PII only for the purpose of providing the Services, and the deliverables under this Agreement. Without limiting the generality of the foregoing, Vendor shall ensure that all agreements entered into between Vendor and it Subcontractor shall contain substantially similar terms and conditions relating to PII as set forth in this Agreement, including safeguards and standards for the protection of the PII at least as strict as those contained in this Section and which will (i) bar any further subcontracting or access to the PII without the written consent of the Customer; and (ii) include a right of Vendor and the Customer to (A) review and audit books and records of such a party relating to the performance of the Services, including, without limitation, books and records containing or relating to the PII; (B) audit and physically inspect the premises of Subcontractor or any premises where the PII is being collected, used, stored, or disclosed in connection with this Agreement, in order to verify compliance with the terms and conditions of such agreements and this Agreement;

- ensure that any Subcontractors' employees receiving or having access to such PII are advised of the terms and conditions relating to PII described above and require such persons to abide by such requirements in writing in a form acceptable to the Customer;
- immediately notify the Customer's representative for the purposes of this Agreement of (a) any legally binding request for disclosure of the PII by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement obligation; (b) any suspected or actual accidental or unauthorized access or disclosure of the PII not expressly contemplated by this Agreement; and (c) any request received directly from an individual without responding to that request, unless he has been otherwise authorized to do so;
- immediately notify the Customer (verbally if necessary and thereafter followed up in writing) if Vendor or a Subcontractor becomes aware of any actual or suspected breach of any of the provisions of this Section and immediately take all necessary measures to investigate and mitigate such breach and prevent further breaches;
- fully cooperate with, and assist in, any investigation by the Customer or any Authority following the approval and direction of the Customer of a complaint that any such PII has been collected, used or disclosed by Vendor or a subcontractor contrary to this Agreement or to the Applicable Privacy Laws;
- allow the Customer or its agents the opportunity to audit Vendor's privacy and data protection practices (including as necessary, its books and records) with respect to PII to ensure compliance with the requirement of this Section 12 and this Agreement more generally, including its data storage facilities for PII (including Vendor's premises or those of subcontractors) and Vendor shall use best efforts to correct any defects observed by the Customer, including the administrative procedures of Vendor, and to otherwise confirm compliance by Vendor with its obligations under this Agreement;
- fully cooperate with the Customer in connection with any investigations, audits or information requests that may be made in connection with Applicable Privacy Laws, including permitting the Customer (or a duly qualified independent auditor or inspection authority selected by the Customer and not reasonably rejected to by Vendor) at Customer's cost to examine and audit (collectively, a "Customer PII Audit") its data storage facilities for PII (including Vendor's premises or those of Subcontractors) with a view to determining the reasons for such security breach and prevent its future occurrence provided that Customer shall (and shall ensure that any auditor or inspection authority carrying out a Customer PII Audit shall) maintain the confidentiality of all PII as required by applicable Privacy Laws and all Confidential Information of Vendor as the Customer is required to do under this Agreement; and
- allow the Customer or its agents the opportunity to audit Vendor's privacy and data protection practices with respect to PII and at its own expense, use its best efforts to correct any defects observed by the Customer, acting reasonably, upon prior written notice, during standard business hours, to review and/or audit the appropriate records directly related to this Agreement, including the

administrative procedures of Vendor, and to otherwise confirm compliance by Vendor with its obligations under this Agreement, including its handling of PII pursuant to this Section.

- On the expiration or termination of this Agreement, Vendor shall complete the procedures outlined in Sections XXX regarding the return and destruction of PII.

- Inquiries. In the event of an Inquiry, Vendor shall immediately notify the Customer. Where Vendor is required to disclose PII as a result of an Inquiry, other than in the form of a response to a request for access or correction, Vendor shall, prior to disclosure where possible, advise the Customer of: (i) the nature of the Inquiry; (ii) who made the Inquiry; (iii) when the Inquiry was received; (iv) what information was sought by and disclosed in response to the Inquiry; and (v) how it plans to respond or has responded to the Inquiry. The Customer shall not be responsible for any costs associated with Vendor's response to an Inquiry.

- Notification of Data Breach. If it knows or suspects that a Data Breach has occurred, Vendor shall immediately notify the Customer and take steps to contain the Data Breach and recover the PII. Vendor shall also comply with all mandatory data breach requirements contained in the Applicable Privacy Laws, including reporting to Authorities such as XXX and individual authorized users as applicable, any breach of security of security safeguards involving PII under its control as soon as feasible after Vendor has determined that the breach has occurred if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. Vendor shall also notify any other organization, government institution or part of a government institution of the breach as soon as feasible after Vendor has determined the breach has occurred if Vendor believes that the other organization, or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm. The notification to the Authority, including XXX, shall contain sufficient information that describes such Data Breach and the notification to individuals shall contain sufficient information to allow the individual to understand the significance to them of the Data Breach and to take steps, if any are possible, to reduce the harm that could result from it or mitigate that harm, as well as any other prescribed information. Vendor shall investigate all Data Breaches and report the results of the investigation to the Customer as soon as feasible after Vendor has determined the breach has occurred. Vendor shall ensure by contract that all of its Subcontractors, contractors and employees are required to: (i) immediately advise it of any Data Breaches in respect of PII in the custody of Subcontractors, contractors and employees; and (ii) promptly investigate and remediate such Data Breaches, and advise Vendor of such investigation and remediation. All costs associated with any investigation and any remedial steps taken by a Subcontractor or contractor shall be the responsibility of Vendor. Where the Customer in its sole discretion considers it appropriate or necessary to participate in or direct any response to a Data Breach, Vendor shall fully cooperate with the Customer at no additional cost to facilitate such participation or comply with such direction, as the case may be. Vendor shall keep and maintain a record of every Data Breach involving PII under its control.

- Accuracy. Vendor shall take reasonable steps to ensure that all PII is as accurate, complete, and up-to-date as necessary for the purposes for which it will be used or disclosed. When it becomes aware of the need to update PII, Vendor shall, within five (5) Business Days, make such update, or shall cause such update to be made, to the PII in its custody or under its control.

- Secure Destruction. Not later than thirty (30) days following the later of (i) any termination or expiration of this Agreement; or (ii) the last day of any post-termination rights period, Vendor shall ensure that at the end of such retention periods, the destruction of records and devices containing PII is carried out in a manner that ensures the security, privacy or confidentiality of the PII, including at minimum: (i) ensuring that any shredding is done by cross-cutting or confetti shredding all paper records; or (ii) wiping or physically destroying electronic records and devices in a manner that ensures that the PII cannot be reconstituted. Where it destroys PII, Vendor shall use an information destruction provider that is certified by the National Association of Information Destruction - Canada or equivalent body and shall, upon request, provide to the Customer an attestation of destruction including the date, time, location and method of destruction and signature of the operator.

- Additional Vendor Indemnities. Vendor shall indemnify and save harmless the Indemnified Parties from any and all losses, costs, damages, liabilities (including any and all liability for damages to property and injury to persons, including death), judgments, claims, demands, causes of action, contracts, suits, actions or other proceedings of any kind or nature and expenses (including legal fees on a solicitor and solicitor's own client basis) that the Indemnified Parties or any of them, may suffer or incur howsoever caused ("Losses") arising out of or in connection with, in any way related to, or as a result of: (a) including any breach by Vendor of its obligations under this Agreement or any breach by Vendor of its representations, warranties and covenants; (b) any violation of Sections X (Confidentiality), X (PII) and (c) any breach of the Requirements of Laws, including Applicable Privacy Laws and any costs, expenses, award of damages or settlement made in relation to any proceedings, complaints, actions or claims made by third parties or individuals, or in relation to compliance by Customer with any orders or directions given against or to Customer by any court or Authority arising from any breach of or non-compliance with Applicable Privacy Laws or the terms and conditions of this Agreement by Vendor in the course of performing any Services or providing deliverables hereunder; to the extent caused by Vendor or Subcontractors, or others for whom Vendor is in law responsible in connection with this Agreement, excluding any Losses caused by the gross negligence or willful misconduct of the Indemnified Parties.