NOVA SCOTIA BARRISTERS' SOCIETY

NOVA SCOTIA BARRISTERS' SOCIETY
CLOUD COMPUTING CHECKLIST

Last Updated on November 15, 2021

CLOUD-BASED SERVICE PROVIDER VERSION (FOR COMPLETION BY PROVIDERS)

*This checklist has been developed for Nova Scotia lawyers and law practices (the "**Law Practice**") to be used when assessing a cloud-based service offered by a cloud-based service provider (the "**Provider(s)**"). Upon receiving this document, it is requested that Providers please complete all questions answering "Yes" or "No" to each and return this document to the Law Practice. In instances where Providers answer "No", please provide an explanation in the Comments box.*

Portions of this checklist have been adapted from The Law Society of Saskatchewan's Cloud Computing Guide.

#	Question	Yes	No	Comments
	INFRASTRUCTURE			
1.	Will Law Practice's cloud data and any backups and related infrastructure be located within Canada?	☐	☐	
2.	Does the Provider have a method to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)?	☐	☐	
3.	Does the Provider backup Law Practice data to a secure offsite location which is compliant with the same data security accreditations as the Provider's production data centre?	☐	☐	
4.	Is cloud data encrypted at all times including on any applicable mobile application, in motion over the Internet, and on the cloud (or at rest) with current encryption algorithms (including appropriate use of client-side vs. server-side encryption) and reviewed periodically?	☐	☐	
5.	Does the Provider utilize company-based security including intrusion detection and prevention and spam and virus filters?	☐	☐	
6.	Does the Provider use VPN or other encryption services for remote administration and are the encryption algorithms reviewed and updated periodically?	☐	☐	

#	Question	Yes	No	Comments
7.	Does the Provider utilize multi-factor/two-factor authentication for remote administration?	☐	☐	
8.	Does the Provider logically isolate Law Practice data from other tenants and management traffic?	☐	☐	
9.	Has the Provider implemented firewalls?	☐	☐	
10.	Does the Provider ensure the cloud-based infrastructure is synchronized with Stratum 1 time servers?	☐	☐	
11.	Does the Provider enforce a limit of logon attempts and concurrent sessions?	☐	☐	
12.	Has the Provider implemented distributed denial of service attack protection?	☐	☐	
13.	Does the Provider provide a service that enables the Law Practice to assess downtime, performance, and other key usage metrics?	☐	☐	
	LEGAL COMPLIANCE AND INDUSTRY BEST PRACTICES			
14.	Is the Provider in compliance with all applicable privacy legislation and regulations in respect the collection, storage and protection of personal information?	☐	☐	
15.	Does the Provider secure remote access according to industry best practices such as encryption of data in transit, security certificates, and two-factor authentication?	☐	☐	
16.	Is the Provider in compliance with a relevant security standard such as NIST CSF, ISO 27001, SOC or PCI DSS as demonstrated via certification with accreditation?	☐	☐	
17.	Is the Provider able to comply with reasonable data access requests when compelled to do so by law?	☐	☐	
18.	Does the Provider implement change controls in accordance with reasonable industry practices including not utilizing production data in test environments?	☐	☐	

#	Question	Yes	No	Comments
19.	Does the Provider secure cloud-based databases using appropriate industry standards and logically isolate information?	☐	☐	
20.	Is the Provider able to retain and/or archive cloud data for any Law Practice specified or legally required period?	☐	☐	
21.	Is the Provider in compliance with at least Level 1 of Cloud Security Alliance (CSA) Security Trust?	☐	☐	
22.	Does the Provider support e-discovery and legal holds to meet the needs of any investigations or judicial requests?	☐	☐	
23.	Does the Provider dispose of assets and information in accordance with industry best practices and provide written confirmation on request? (with the exception of backups)	☐	☐	
	INTERNAL POLICIES AND PROCESSES			
24.	Does the Provider have a policy and process to handle ransomware attacks?	☐	☐	
25.	Does the Provider have a disaster recovery/business continuity plan including the ability, on request, to courier client data on a secure hard drive in the event of an outage or local system failure?	☐	☐	
26.	Are the Provider's backup and recovery procedures documented in its disaster recovery plan and tested at least annually and approved by management?	☐	☐	
27.	When Provider conducts a security investigation for a potential breach does it retain an investigation report for a period of at least two years thereafter?	☐	☐	
28.	Does the Provider maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts?	☐	☐	
29.	Does the Provider conduct security awareness and training for its employees at least annually (including phish testing)?	☐	☐	

#	Question	Yes	No	Comments
30.	Does the Provider retain usage logs that are sufficiently detailed to determine who did what on the cloud service for a period of 90 days?	☐	☐	
31.	Does the Provider provide appropriate Law Practice access to the aforementioned logs on request?	☐	☐	
32.	Does the Provider correlate, monitor and alert on the aforementioned logs?	☐	☐	
33.	Does the Provider enforce password length, complexity and history for password-based authentication on its employees?	☐	☐	
34.	Does the Provider conduct vulnerability scans and penetration tests at least annually and for new systems and material changes to existing ones?	☐	☐	
35.	Does the Provider utilize access-based security based on the identity or role of the individual within its organization which addresses onboarding, off-boarding, transition between roles, regular access reviews, and limit and control use of administrator privileges and inactivity timeouts?	☐	☐	
	SUPPORT			
36.	Does the Provider offer standard technical support during normal working hours?	☐	☐	
37.	Does the Provider offer emergency technical support outside of normal working hours?	☐	☐	
38.	Does the Provider offer an extensive knowledge base on the cloud service for self-help and support?	☐	☐	
39.	In the event Law Practice discontinues its use of the service, will Provider provide Law Practice's cloud data in a format that can be moved to another cloud provider?	☐	☐	
40.	Will the Provider provide transition support if Law Practice elects to terminate use of the cloud-based service?	☐	☐	

#	Question	Yes	No	Comments
41.	Does the Provider support single sign-on technologies for authentication?	☐	☐	
	AGREEMENT TERMS			
42.	Does the Provider's form of License Agreement (the "**Agreement**") provide that the Provider shall not share any of Law Practice's cloud data with other parties nor utilize any subcontractors or third-party cloud service providers without the prior written consent of the Law Practice?	☐	☐	
43.	Does the Agreement ensure that ownership in any intellectual property rights to any cloud data are not transferred during the life of the contract and thereafter?	☐	☐	
44.	Does the Agreement require the Provider to notify Law Practices of any security breaches that could affect their cloud data within 48 hours of discovery of the breach?	☐	☐	
45.	Does the Agreement require the Provider to provide Law Practice with reasonable notice prior to any planned outages for maintenance?	☐	☐	
46.	Does the Agreement require the Provider to provide prior written notice to Law Practices upon a change to the Agreement or any other underlying policies?	☐	☐	
47.	Does the Provider provide representations in the Agreement on the availability, performance and bandwidth of the cloud service, including uptime and time required to restore backups?	☐	☐	
48.	Does the Agreement provide for any financial penalties payable to the Law Practice in the event the Provider fails to comply with the aforementioned representations?	☐	☐	
49.	Does the Agreement require the Provider to carry liability insurance associated with ransomware attacks or cyber security risk?	☐	☐	
50.	Does the Agreement provide that in the event Law Practice's cloud data is disclosed to a third party in breach of Provider's obligations will Provider compensate Law Practice for their losses?	☐	☐	

#	Question	Yes	No	Comments
51.	Does the Agreement provide that there is no cap on Provider's liability to Law Practices as a result of losses resulting from a data breach?	☐	☐	

NOVA SCOTIA
BARRISTERS' SOCIETY

NOVA SCOTIA BARRISTERS' SOCIETY
CLOUD COMPUTING CHECKLIST

Last Updated on November 15, 2021

ANNOTATED LAW PRACTICE VERSION (FOR USE BY LAW PRACTICE'S ONLY)

*This checklist has been developed for Nova Scotia lawyers and law practices (the "**Law Practice**") to be used when assessing a cloud-based service offered by a cloud-based service provider (the "**Provider(s)**"). There are two versions of this checklist. This "Annotated Law Practice Version" is intended to be used by the Law Practice only to interpret and assess the answers provided by the Provider after it has completed the "Service Provider Version". Ideally, a Provider would answer "Yes" to each of the provided questions, but as is provided below, there are instances where a "No" answer may be permissible. In this version, commentary has been provided to assist the Law Practice's in determining when a "No" answer could be acceptable. For ease of use, this checklist has been organized into five sections. The earlier sections are more technical in nature while the later ones are less technical and more general. For the more technical sections, and if the provided commentary does not provide the Law Practice with sufficient comfort, it is recommended to consult with a computer security expert or managed service provider if particularly sensitive data is being stored.*

Portions of this checklist have been adapted from The Law Society of Saskatchewan's Cloud Computing Guide.

#	Question	Yes	No	Comments
	INFRASTRUCTURE *The following questions are technical in nature. Some Law Practices will not be aware of the meaning of these questions, but most sophisticated Providers should be able to provide "Yes" to most, if not all, of the questions. Given the technical nature of these questions, it may be advisable to consult with a computer security expert or managed service provider the Provider does not answer "Yes" to the critical questions.*			
1.	Will Law Practice's cloud data and any backups and related infrastructure be located within Canada?	☐	☐	*Should generally be "Yes", but it would be permissible in the EU in most cases, but the US isn't recommended because of government based compliance policies (PIPEDA). May also be permissible if backups are encrypted.*
2.	Does the Provider have a method to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)?	☐	☐	*Always "Yes"*

#	Question	Yes	No	Comments
3.	Does the Provider backup Law Practice data to a secure offsite location which is compliant with the same data security accreditations as the Provider's production data centre?	☐	☐	*Always "Yes"*
4.	Is cloud data encrypted at all times including on any applicable mobile application, in motion over the Internet, and on the cloud (or at rest) with current encryption algorithms (including appropriate use of client-side vs. server-side encryption) and reviewed periodically?	☐	☐	*Always "Yes". Generally speaking, client-side encryption prevents any third parties from viewing the unencrypted version of the data where server-side encryption enables the Provider to access the data.*
5.	Does the Provider utilize company-based security including intrusion detection and prevention and spam and virus filters?	☐	☐	*Always "Yes".*
6.	Does the Provider use VPN or other encryption services for remote administration and are the encryption algorithms reviewed and updated periodically?	☐	☐	*Always "Yes"*
7.	Does the Provider utilize multi-factor/two-factor authentication for remote administration?	☐	☐	*Always "Yes"*
8.	Does the Provider logically isolate Law Practice data from other tenants and management traffic?	☐	☐	*Always "Yes"*
9.	Has the Provider implemented firewalls?	☐	☐	*Always "Yes"*
10.	Does the Provider ensure the cloud-based infrastructure is synchronized with Stratum 1 time servers?	☐	☐	*Any major vendor or datacentre should have such a time server in place particularly where the service covers core business services (such as email, documents, or communications) but not having such a time server may be permissible for non-core activities (non-client materials, legal research, or reference materials).*
11.	Does the Provider enforce a limit of logon attempts and concurrent sessions?	☐	☐	*Should generally be "Yes" in most cases – particularly with larger cloud-based vendors but may be permissible for non-core services*

#	Question	Yes	No	Comments
12.	Has the Provider implemented distributed denial of service attack protection?	☐	☐	*This should be "Yes" for core business services but may be permissible for non-core business services*
13.	Does the Provider provide a service that enables the Law Practice to assess downtime, performance, and other key usage metrics?	☐	☐	*If Service Provider agrees to promptly notify the Law Practice if issues arise then "No" is acceptable*
	LEGAL COMPLIANCE AND INDUSTRY BEST PRACTICES *The following questions are somewhat technical and aim to ensure that the Provider follows applicable laws, standards and industry best practices. Assessing these questions can be challenging since the adoption of these technical standards varies across the industry and the type of cloud service, and many are in a state of flux given the evolving nature of cloud-based technologies. This is another section where the assistance of a computer security expert or managed service provider may be advisable.*			
14.	Is the Provider in compliance with all applicable privacy legislation and regulations in respect the collection, storage and protection of personal information?	☐	☐	*Always "Yes"*
15.	Does the Provider secure remote access according to industry best practices such as encryption of data in transit, security certificates, and two-factor authentication?	☐	☐	*Always "Yes"*
16.	Is the Provider in compliance with a relevant security standard such as NIST CSF, ISO 27001, SOC or PCI DSS as demonstrated via certification with accreditation?	☐	☐	*Always "Yes". SOC is always critical. PCI is critical for credit card information. NIST CSF and ISO are important from a business perspective on how to handle security protocols (largely interchangeable).*
17.	Is the Provider able to comply with reasonable data access requests when compelled to do so by law?	☐	☐	*Always "Yes"*
18.	Does the Provider implement change controls in accordance with reasonable industry practices including not utilizing production data in test environments?	☐	☐	*Always "Yes"*
19.	Does the Provider secure cloud-based databases using appropriate industry standards and logically isolate information?	☐	☐	*Always "Yes"*

#	Question	Yes	No	Comments
20.	Is the Provider able to retain and/or archive cloud data for any Law Practice specified or legally required period?	☐	☐	*Ideally "Yes", but Providers may not know the specified period so at a minimum should disclose how long they retain or archive such data and such time period should be acceptable to the Law Practice*
21.	Is the Provider in compliance with at least Level 1 of Cloud Security Alliance (CSA) Security Trust?	☐	☐	*Preferable but not always strictly required if ISO or a similar standard in place.*
22.	Does the Provider support e-discovery and legal holds to meet the needs of any investigations or judicial requests?	☐	☐	*This may not always be a "Yes" since their infrastructure may not be such that would allow such support, but Law Practices should be aware of any such limitations.*
23.	Does the Provider dispose of assets and information in accordance with industry best practices and provide written confirmation on request? (with the exception of backups)	☐	☐	*If Provider isn't storing confidential information then "No" may be permissible. However, if storing confidential information then should always be "Yes".*
	INTERNAL POLICIES AND PROCESSES *The following questions relate to the Provider's internal policies and processes intended to ensure that the Provider has systems in place to mitigate the risks of storing data in the cloud. Even if the Provider has a robust security infrastructure, it is important that they effectively manage that infrastructure with supporting policies and processes. The vast majority of Providers should be able to answer "Yes" to each of these questions (and in particular if they are compliant with the aforementioned industry standards and certifications which would require many such policies and processes to be in place).*			
24.	Does the Provider have a policy and process to handle ransomware attacks?	☐	☐	*Always "Yes"*
25.	Does the Provider have a disaster recovery/business continuity plan including the ability, on request, to courier client data on a secure hard drive in the event of an outage or local system failure?	☐	☐	*Always "Yes"*
26.	Are the Provider's backup and recovery procedures documented in its disaster recovery plan and tested at least annually and approved by management?	☐	☐	*Always "Yes"*

#	Question	Yes	No	Comments
27.	When Provider conducts a security investigation for a potential breach does it retain an investigation report for a period of at least two years thereafter?	☐	☐	*Always "Yes"*
28.	Does the Provider maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts?	☐	☐	*Always "Yes"*
29.	Does the Provider conduct security awareness and training for its employees at least annually (including phish testing)?	☐	☐	*Always "Yes"*
30.	Does the Provider retain usage logs that are sufficiently detailed to determine who did what on the cloud service for a period of 90 days?	☐	☐	*Always "Yes"*
31.	Does the Provider provide appropriate Law Practice access to the aforementioned logs on request?	☐	☐	*Always "Yes"*
32.	Does the Provider correlate, monitor and alert on the aforementioned logs?	☐	☐	*Always "Yes"*
33.	Does the Provider enforce password length, complexity and history for password-based authentication on its employees?	☐	☐	*Always "Yes"*
34.	Does the Provider conduct vulnerability scans and penetration tests at least annually and for new systems and material changes to existing ones?	☐	☐	*Always "Yes"*
35.	Does the Provider utilize access-based security based on the identity or role of the individual within its organization which addresses onboarding, off-boarding, transition between roles, regular access reviews, and limit and control use of administrator privileges and inactivity timeouts?	☐	☐	*Should generally be "Yes", but if there is no access to confidential or sensitive data on the service it may be permissible to not maintain these security standards*
	SUPPORT *The following questions relate to the support offered to the Law Practice by the Provider both during the use of the cloud service and in the event of a discontinuance of use or transition to an alternative. These questions are not particularly technical in nature and Law Practices will need to satisfy themselves to the support provided given the nature of the service being provided.*			
36.	Does the Provider offer standard technical support during normal working hours?	☐	☐	*Always "Yes"*

#	Question	Yes	No	Comments
37.	Does the Provider offer emergency technical support outside of normal working hours?	☐	☐	*Always "Yes"*
38.	Does the Provider offer an extensive knowledge base on the cloud service for self-help and support?	☐	☐	*Should be "Yes" in most cases – particularly with larger cloud-based vendors*
39.	In the event Law Practice discontinues its use of the service, will Provider provide Law Practice's cloud data in a format that can be moved to another cloud provider?	☐	☐	*Should generally be "Yes", but depends on whether the nature of the data requires the ability to transfer it to another provider. Law Practices should expect to have to pay for this service in some cases.*
40.	Will the Provider provide transition support if Law Practice elects to terminate use of the cloud-based service?	☐	☐	*This is nice to have but whether this is critical depends on the nature of the data and whether transition support would be required*
41.	Does the Provider support single sign-on technologies for authentication?	☐	☐	*Provided Law Practice has strong password policies in place this is more of a convenience and is likely permissible to be "No"*
	AGREEMENT TERMS *The following questions are less technical in nature and serve as a list of contractual terms that should be considered by the Law Practice when reviewing the Provider's form of License Agreement (the "**Agreement**"). While some Law Practices may elect to ask these questions of the Provider directly, they can also be ascertained through a review of the Agreement. In many instances, particularly when dealing with large and well-established service providers, the Provider may have minimal flexibility or willingness to revise their standard form agreement. As a result, it is recommended that Law Practices utilize these questions to satisfy themselves on the associated risks of "No" answers under the Agreement acknowledging that it may not be feasible to have "Yes" answers for all questions.*			
42.	Does the Provider's form of License Agreement (the "**Agreement**") provide that the Provider shall not share any of Law Practice's cloud data with other parties nor utilize any subcontractors or third-party cloud service providers without the prior written consent of the Law Practice?	☐	☐	*Always "Yes"*

#	Question	Yes	No	Comments
43.	Does the Agreement ensure that ownership in any intellectual property rights to any cloud data are not transferred during the life of the contract and thereafter?	☐	☐	*Always "Yes"*
44.	Does the Agreement require the Provider to notify Law Practices of any security breaches that could affect their cloud data within 48 hours of discovery of the breach?	☐	☐	*Always "Yes"*
45.	Does the Agreement require the Provider to provide Law Practice with reasonable notice prior to any planned outages for maintenance?	☐	☐	Always "Yes"
46.	Does the Agreement require the Provider to provide prior written notice to Law Practices upon a change to the Agreement or any other underlying policies?	☐	☐	*Ideally "Yes", though in some instances the Provider may incorporate by reference general terms of service that are published on their website from time to time. If the Provider doesn't agree to provide notice then it is recommended that Law Practices periodically check any such published terms*
47.	Does the Provider provide representations in the Agreement on the availability, performance and bandwidth of the cloud service, including uptime and time required to restore backups?	☐	☐	*Should generally be representations to this effect but Law Practice should be comfortable with the standards that have been set*
48.	Does the Agreement provide for any financial penalties payable to the Law Practice in the event the Provider fails to comply with the aforementioned representations?	☐	☐	*More of a legal question which a Law Practice will need to be comfortable with*
49.	Does the Agreement require the Provider to carry liability insurance associated with ransomware attacks or cyber security risk?	☐	☐	*More of a legal question, but most vendors should if particularly sensitive data is stored in the cloud service*
50.	Does the Agreement provide that in the event Law Practice's cloud data is disclosed to a third party in breach of Provider's obligations will Provider compensate Law Practice for their losses?	☐	☐	*Most vendors will likely say "No" to this anyway (though some may cover the cost of the service). This is more intended to ensure that Law Practices are aware of the risks and prepared to assume them.*

#	Question	Yes	No	Comments
51.	Does the Agreement provide that there is no cap on Provider's liability to Law Practices as a result of losses resulting from a data breach?	☐	☐	*Most vendors will likely say "No" to this and will almost certainly place a cap on liability. This is more intended to ensure that Law Practices are aware of the risk they are assuming.*