**Cloud Computing Checklist**

**Cloud-Based Service Provider Version (for completion by providers)**

This checklist was 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 comment box.

Portions of this checklist are adapted from The Law Society of Saskatchewan’s Cloud Computing Guide.

| **#** | **Question** | **Yes** | **No** | **Comments** |
| --- | --- | --- | --- | --- |
| **INFRASTRUCTURE** | | | | |
|  | Will Law Practice’s cloud data and any backups and related infrastructure be located within Canada? |  |  |  |
|  | Does the Provider have a method to monitor for and report abuse of the cloud service (e.g. Denial-of-Service attacks)? |  |  |  |
|  | 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? |  |  |  |
|  | 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? |  |  |  |
|  | Does the Provider utilize company-based security including intrusion detection and prevention and spam and virus filters? |  |  |  |
|  | Does the Provider use VPN or other encryption services for remote administration and are the encryption algorithms reviewed and updated periodically? |  |  |  |
|  | Does the Provider utilize multi-factor/two-factor authentication for remote administration? |  |  |  |
|  | Does the Provider logically isolate Law Practice data from other tenants and management traffic? |  |  |  |
|  | Has the Provider implemented firewalls? |  |  |  |
|  | Does the Provider ensure the cloud-based infrastructure is synchronized with Stratum 1-time servers? |  |  |  |
|  | Does the Provider enforce a limit of logon attempts and concurrent sessions? |  |  |  |
|  | Has the Provider implemented distributed denial of service attack protection? |  |  |  |
|  | 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** | | | | |
|  | Is the Provider in compliance with all applicable privacy legislation and regulations in respect the collection, storage and protection of personal information? |  |  |  |
|  | Does the Provider secure remote access according to industry best practices such as encryption of data in transit, security certificates, and two-factor authentication? |  |  |  |
|  | 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? |  |  |  |
|  | Is the Provider able to comply with reasonable data access requests when compelled to do so by law? |  |  |  |
|  | Does the Provider implement change controls in accordance with reasonable industry practices including not utilizing production data in test environments? |  |  |  |
|  | Does the Provider secure cloud-based databases using appropriate industry standards and logically isolate information? |  |  |  |
|  | Is the Provider able to retain and/or archive cloud data for any Law Practice specified or legally required period? |  |  |  |
|  | Is the Provider in compliance with at least Level 1 of Cloud Security Alliance (CSA) Security Trust? |  |  |  |
|  | Does the Provider support e-discovery and legal holds to meet the needs of any investigations or judicial requests? |  |  |  |
|  | 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** | | | | |
|  | Does the Provider have a policy and process to handle ransomware attacks? |  |  |  |
|  | 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? |  |  |  |
|  | Are the Provider’s backup and recovery procedures documented in its disaster recovery plan and tested at least annually and approved by management? |  |  |  |
|  | Does the Provider have a documented process that activates in the event of a potential security or privacy breach? |  |  |  |
|  | 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? |  |  |  |
|  | 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? |  |  |  |
|  | Does the Provider conduct security awareness and training for its employees at least annually (including phish testing)? |  |  |  |
|  | 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? |  |  |  |
|  | Does the Provider provide appropriate Law Practice access to the aforementioned logs on request? |  |  |  |
|  | Does the Provider correlate, monitor and alert on the aforementioned logs? |  |  |  |
|  | Does the Provider enforce password length, complexity and history for password-based authentication on its employees? |  |  |  |
|  | Does the Provider conduct vulnerability scans and penetration tests at least annually and for new systems and material changes to existing ones? |  |  |  |
|  | 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** | | | | |
|  | Does the Provider offer standard technical support during normal working hours? |  |  |  |
|  | Does the Provider offer emergency technical support outside of normal working hours? |  |  |  |
|  | Does the Provider offer an extensive knowledge base on the cloud service for self-help and support? |  |  |  |
|  | 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? |  |  |  |
|  | Will the Provider provide transition support if Law Practice elects to terminate use of the cloud-based service? |  |  |  |
|  | Does the Provider support single sign-on technologies for authentication? |  |  |  |
| **AGREEMENT TERMS** | | | | |
|  | 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? |  |  |  |
|  | 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? |  |  |  |
|  | 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? |  |  |  |
|  | Does the Agreement require the Provider to provide Law Practice with reasonable notice prior to any planned outages for maintenance? |  |  |  |
|  | 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? |  |  |  |
|  | 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? |  |  |  |
|  | 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? |  |  |  |
|  | Does the Agreement require the Provider to carry liability insurance associated with ransomware attacks or cyber security risk? |  |  |  |
|  | 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? |  |  |  |
|  | 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? |  |  |  |