INFORMATION SECURITY REQUIREMENTS

Contents

[Purpose 2](#_Toc15972631)

[A. Security Policy 2](#_Toc15972632)

[B. Organization of Information Security 3](#_Toc15972633)

[C. Human Resources Security 3](#_Toc15972634)

[D. Account and Password Management 4](#_Toc15972635)

[E. Authorization and Application Controls 4](#_Toc15972636)

[F. Host Security 4](#_Toc15972637)

[G. Network Security 5](#_Toc15972638)

[H. Data Protection 5](#_Toc15972639)

[I. Physical Access 5](#_Toc15972640)

[J. Incident Management and Breach Notice 6](#_Toc15972641)

[K. Business Continuity 6](#_Toc15972642)

[L. Risk Assessment and Treatment 6](#_Toc15972643)

[M. Legal Compliance and Security Posture 7](#_Toc15972644)

[Exhibit 1: Confidentiality and Non-Disclosure Agreement 8](#_Toc15972645)

[Exhibit 2: Incident Notice Requirements 11](#_Toc15972646)

[Primary Contact 11](#_Toc15972647)

[Secondary Contact 11](#_Toc15972648)

# Purpose

\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Client**”) maintains a comprehensive security program to protect Client’s employees, customers, assets, intellectual property, information, and data and has established minimum requirements for information security practices for its vendors and service providers. To protect its relevant assets and data, Client expects law firms providing services to Client (“**Services**”) have practices and procedures that comply with these minimum requirements.

This Information Security Requirements document sets forth Client’s minimum information security and infrastructure policies (the “**Information Security Requirements**”) to be effective as of the date of their acknowledgement by the law firm handling legal matters for Client (“**Firm**”). These Information Security Requirements describe the practices the Firm must meet and maintain in order to protect Client’s Data from possible Security Breach (both as defined below) during the Firm’s provision of Services and for any period of time thereafter during which the Firm has possession of or access to Client Data.

If there are discrepancies between these Information Security Requirements and the underlying engagement letter in place with the Firm (“**Engagement Letter**”), these Information Security Requirements will control.

**Client Data** shall mean Client’s intellectual property, data, software, applications, personally identifiable information, confidential information (both Client’s as well as belonging to a third party, but entrusted to Client), and other assets (“**Information**”) that are in the Firm’s possession or are used, hosted, stored, maintained, processed, reproduced, developed, or transmitted by the Firm in connection with the provision of Services, including Information that is created by the Firm for Client in the course of providing or performing Services for Client.

**Firm Supporting Parties** shall mean the Firm and every current or former, direct or indirect subordinate or non-subordinate employees, contract workers, third-party vendors, agents, subcontractors, including advisers, shareholders and/or partners of the Firm, who are involved in carrying out instructions on behalf of the Firm for Client.

**Resources** shall mean computing resources used to process, store, host, support, or maintain Client Data or on which Client’s applications will be stored.

**Security Breach** shall mean (A) any circumstance pursuant to which applicable law requires notification of such circumstance to be given to affected parties or requires other activity in response to such circumstance; or (B) any actual or attempted compromise of the Firm’s physical security or of the Firm’s systems’ security, resulting in unauthorized access to or possession, acquisition, use, disclosure, theft, safekeeping, manipulation, processing, or reproduction of Client Data.

**Services** shall mean the services or service level agreement described in the Engagement Letter.

Capitalized terms used, but not otherwise defined in these Information Security Requirements have the respective meanings given in the Engagement Letter.

#  Security Policy

1. The Firm has an information security policy that is communicated it to all Firm Supporting Parties (“**Firm Information Security Policy**”). The Firm Information Security Policy specifies policies regarding practices for acceptable possession, acquisition, use, access, disclosure, theft, manipulation, processing, reproduction, maintenance, hosting, safekeeping, or protection of the Firm’s Resources that will store Client Data and of data entrusted to the Firm, including Client Data, that ensure the confidentiality, availability, security, and integrity of the Resources and all such Client Data (“**Firm’s Information Security Safeguards**”). The firm will take punitive actions against Firm Supporting Parties when such policies are not followed.
2. Upon request, the Firm shall make available to Client the Firm’s Information Security Policy.
3. The Firm shall adhere to Information security best practices as derived from International Organization for Standardization 27002.
4. Information Security practices shall be documented and kept current in regards to changes in applicable law, best practices, and industry standards.
5. The Firm has apublished acceptable use policy for all assets used in the provisioning of services to Client.
6. The Firm has third-party contractual agreements in place that comply with the provisions of these Information Security Requirements (or equivalents thereof) as applicable to Client Data. The Firm maintains appropriate safeguards and service delivery levels for subcontracted services.

#  Organization of Information Security

1. The Firm has personnel responsible for information security practices.
2. This resource is responsible for coordinating the Firm’s information security activities such as incident response, third-party access, and setting security best practices based on industry-accepted standards for law firms in your jurisdiction.
3. The Firm represents that appropriate due care and due diligence are being or, if a new engagement, will be exercised, to ensure the protection, confidentiality, maintenance, storage, safekeeping, availability, and integrity of Client Data.

#  Human Resources Security

1. The Firm executes background verification, criminal record check, and/or other pre-employment screening of all Firm Supporting Parties as dictated by the laws and regulations of the Firm’s residence jurisdiction and industry best practices (“**Screening**”). The Firm shall only allow individuals who have passed all such Screening to provide Services to Client.
2. The Firm maintains with all Firm Supporting Parties confidentiality and non-disclosure obligations, with terms and conditions no less restrictive than the non-disclosure and non-use provisions in the form attached hereto as Exhibit 1.
3. The Firm shall remove access rights to Client Data from all Firm Supporting Parties who have been terminated within twenty-four (24) hours of their termination.
4. The Firm provides information security awareness training to all Firm Supporting Parties no less frequently than once per year.
5. The Firm certifies that each Firm Supporting Party completes training on the Firm’s code of conduct governing the secure use of technology and confidentiality of the Firm’s clients’ data and that such training requires acknowledgement that the Firm Supporting Party has been trained and shall comply with the requirements of the Firm’s Information Security Safeguards.

#  Account and Password Management

1. The Firm provides a means to force periodic password changes for Firm Supporting Parties.
2. The Firm enforces a password management policy for Firm Supporting Parties with the following provisions, or offering more protection:
	1. Passwords change within ninety (90) days
	2. Reuse of at least the last five (5) passwords is prohibited
	3. Account lock out after no more than five (5) consecutive failed authentication attempts
	4. Password length of at least eight (8) characters
		1. Required inclusion of a combination of no less than three (3) of the following character types:
			1. Lower case
			2. Upper case
			3. Numbers
			4. Special characters

#  Authorization and Application Controls

1. The Firm shall limit access to Client Data to Firm Supporting Parties who have a need to access Client Data in connection to the uses permitted by these Information Security Requirements.
2. The Firm is responsible for any failure of all Firm Supporting Parties to comply with these terms and conditions regarding Client Data.
3. The Firm agrees to assign minimal access privileges to Firm Supporting Parties when assigning access to Resources containing Client Data or Resources that are used to manage Client Data.
4. The Firm shall perform a minimum of annual reviews of all Resources regarding administrator access used to support Client Data.
5. With regard to the Client Data, the Firm agrees to segregate duties to ensure separation of privileged-access requestors from approvers.

#  Host Security

1. The Firm has tools implemented to detect and remediate software viruses and other malware on all Resources.
2. The Firm implements host intrusion detection/prevention services covering all Resources.
3. The Firm shall prevent administratiion of all hosts and software Resources from being accessed from outside the Firm’s network.
4. The Firm performs vulnerability assessments for all hosts and hardware Resources on an annual basis.
5. The Firm has implemented or will implement, for a new engagement, a security patch and vulnerability management process for all Resources, and operating systems (“**OS**”) and applications. The Firm represents that OS and application security patches are applied within thirty (30) days of such patches being made available from the relevant vendor.
6. The Firm follows a practice of annual third-party penetration testing and application security scans of all Resources.
7. The Firm implements logging for all Resources hosting Client Data.

#  Network Security

1. The Firm has implemented firewalls, intrusion detection, and other network protection services in accordance with IT industry best practices for securing Resources and Client Data.
2. The Firm implements network segmentation on all Resources, OSs, and applications supporting Client Data to limit the effect of any security compromise.

.

1. The Firm identifies and removes all unnecessary services in a timely manner.
2. The Firm and Firm Supporting Parties implement industry best practices to secure remote and wireless connectivity, including strong authentication and encryption.
3. The Firm implements network time protocol (“**NTP**”) for all Resources.

#  Data Protection

1. The Firm agrees to employ industry standard off-the-shelf encryption on laptops and desktops to protect all Client Data stored or transmitted on such laptops and desktops and to securely store or escrow all data encryption keys used in the storage or transmittal of Client Data. The Firm shall ensure the privacy, integrity, and confidentiality of Client Data in its transmission, using verifiable industry-standard tools, education, and practices for law firms in your jurisdiction.
2. The Firm agrees to employ industry-standard encryption protecting any Client Data in storage or in transit.
3. All application and infrastructure passwords shall be changed from default settings prior to implementation.
4. All Client Data shall be encrypted when transferred to backup storage and other portable devices unless otherwise required by a court or government or unless consented to by Client. Only strong ciphers (symmetric key length at least 128 bits) shall be utilized where Client Data is encrypted for storage or transmittal.
5. The Firm agrees to provide three (3) months of notice before the Firm transmits any Client Data outside the EU to provide an opportunity for Client to agree in writing before any Client Data is moved to such location. Client reserves the right to terminate the Engagement Letter, with thirty (30) days’ notice should Client be unable to approve the transmission.
6. The Firm shall provide a summary of how Client Data held by the Firm will be retained and destroyed on Exhibit 3 of these Information Security Guidelines. After its retention of data period of time, the Firm shall destroy all Client Data stored on hosted infrastructure, databases, Resources, and backup storage media.

#  Physical Access

1. The Firm enforces badge access with both photo and electronic verification with logging to both physical premises and data centers hosting Client Data and applications.
2. The Firm uses 24x7 camera monitoring to monitor its office’s entrance and egress points.
3. The Firm uses physical intrusion and fire alarms in all areas where Client business is conducted.
4. The Firm logs physical access to all facilities and data centers hosting Client Data and applications.
5. The Firm shall ensure doors to secure areas containing Client Data remain locked.

#  Incident Management and Breach Notice

1. The Firm has and follows a documented security incident response plan. In the event of any incident affecting Client Data, an application managing Client Data, or other Client assets under the Firm’s control, the Firm agrees to notify Client, in writing, of such event consistent with the incident classification, contacts, and timing described in the Incident Notice Requirements in Exhibit 2 of these Information Security Requirements.
2. If such incident were to occur, the Firm shall designate a single point of contact within the Firm’s organization for Client to work with. This point of contact shall initiate and manage regular incident status calls between the Firm, Client, any Firm Supporting Parties, and any other involved parties.
3. In the event of a security breach, as necessary, the Firm shall engage a third party of sufficient reputation to manage the response and remediation. A third-party penetration test must be performed after corrective actions are implemented and the test results shall be promptly provided to Client.

#  Business Continuity

1. The Firm shall backup Client applications, data, and software on a regular basis, no less frequently than weekly.
2. The Firm shall have a managed disaster recovery program by which all Resources and supporting infrastructure for Client applications and Client Data are available and supported. This shall include, but is not limited to, storage capacity, processing power, points of presence, power generators, and backup power.

# Risk Assessment and Treatment

1.The Firm regularly performs security risk assessments for all Resources and infrastructure used to present, manage, or otherwise sustain Client Data.

2.The Firm shall analyze, remediate, and document identified risks using industry-accepted risk mitigation strategies, such as risk avoidance, risk reduction, risk retention, and risk transfer.

3.The Firm shall retain risk assessment documents for risk accountability for no less than two (2) years, unless consented to otherwise in writing by Client or its representative.

#  Legal Compliance and Security Posture

1. The Firm certifies that the Firm’s Information Security Safeguards at all times comply with applicable laws in the Firm’s jurisdiction.
2. The Firm agrees to require industry-accepted security safeguards from any third-party subcontracted services that work with Client Data and to require that such third-party subcontracted services will notify Client in writing before moving any Client Data to any third party or across national boundaries.
3. The Firm provides Client with the right to audit the Firm’s compliance with these Information Security Requirements . Client shall provide the Firm a minimum of thirty (30) days’ notice prior to any audit.

IN WITNESS WHEREOF, the Firm has duly executed these Information Security Requirements as of the date signed below.

The Firm Name:

Signature:

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title:

Date:

# Exhibit 1: Confidentiality and Non-Disclosure Agreement

MUTUAL CONFIDENTIALITY AGREEMENT

# Exhibit 2: Incident Notice Requirements

|  |  |  |
| --- | --- | --- |
| Incident | **CONTACT(S)** | **TIMING** |
| Security Breach affecting Client Data, systems containing Client Data, or systems on the same network as systems containing Client Data.  | Via \_\_\_\_\_\_\_\_ and by phone to the primary contacts listed below | Within 24 hours of initial detection of breach |

# Primary Contact

Name:

Phone:

Email:

# Secondary Contact

Name:

Position: Director of Information Security

Location:

Phone:

Email:

# Exhibit 3: Summary of How Client Data held by the Firm will be retained and destroyed