The Association of Corporate Counsel (ACC) and a group of its members have developed this *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information ("Model Controls")* to help in-house counsel as they set expectations with their outside vendors, including outside counsel, regarding the types of data security controls these vendors should employ to protect their company 's confidential information. The Model Controls provide a list of baseline security measures and controls some legal departments may consider requiring from outside vendors. It is ACC's hope that the Model Controls offer in-house counsel a streamlined and consistent approach to setting expectations with respect to the data security practices of their outside vendors.

This document does not constitute legal advice or legal opinion on specific facts, and it is not intended to be a definitive statement on the subject but rather serves as a resource providing practical information to in-house counsel. This document is not a substitute for corporate counsel's own legal analysis and good judgment; company's internal requirements and policies; or regulatory provisions. Further, this document is not intended to establish any industry standards for any purpose for either the company client or the outside vendor, including, but not limited to, contract, professional malpractice, or negligence.

MODEL INFORMATION PROTECTION AND SECURITY CONTROLS FOR OUTSIDE COUNSEL POSSESSING COMPANY CONFIDENTIAL INFORMATION

Definition of "Company Confidential Information":

"Company Confidential Information" is defined as any information that is proprietary to Company and is not publicly available including, without limitation, information that is:

- Attorney-client privileged;
- Confidential information, which, if disclosed, could cause damage to the interests of Company;
- Material non-public information concerning publicly traded corporations;
- Personally Identifiable Information ("PII*") for any Company employee, contractor, customer, or supplier. For the purpose of this document, PII is defined as information that can be used to identify, contact, or locate a natural person, including, without limitation, a Company customer or website user, natural person's name, IP address, email address, postal address, telephone number, account numbers, date of birth, driver's license or other government-issued identification card numbers and social security numbers, or any other information that is linked or linkable to an individual.
- Protected Health Information ("PHI") shall have the same meaning as the term "protected health information" at 45 C.F.R.§160.103;
- Information relating to the physical security of Company operations;
- Information relating to the Company's cyber security;
- Information from any source that may tend to incriminate the Company, subject the company to fines or penalties, form the basis for litigation against the company, or which may tend to damage the Company's reputation or the reputation of its officers, directors, employees, or agents;
- Information that is legally required to be protected under the laws applicable to the company data.

1. Policies and Procedures

Outside Counsel shall have in place appropriate organizational and technical measures to protect Company Confidential Information or other information of a similar nature

against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and nature of the information to be protected. Outside Counsel shall have in place internal security and privacy policies designed to protect the security, confidentiality, and integrity of Company Confidential Information or other information of a similar nature that include: security policy; organization of information security; asset management; human resources security; physical and environment security; communications and operations management; access control; information systems acquisition, development, and maintenance; information security incident management; business continuity management; personnel training; and compliance.

Outside Counsel shall have incident and problem management procedures that allow for the reasonable investigation, response, mitigation, and notification of events that implicate the confidentiality, integrity, and availability of Outside Counsel's technology and information assets, or events that cause the unauthorized or unintentional disclosure of Company Confidential Information. Outside Counsel will review at least annually its incident response and problem management procedures to ensure they are fit for purpose.

Outside Counsel shall have adequate resources and management oversight to ensure the proper development and maintenance of information security and technology policies, procedures, and standards throughout the course of their relationship with Company. Outside Counsel shall provide and maintain information security training for all employees and provide a summary of such training to Company upon request.

2. Retention and Return/Destruction

2.1 Retention

Outside Counsel shall retain Company Confidential Information only for as long as specified by Company for the matter(s) on which Outside Counsel is working or as otherwise necessary to satisfy the purposes for which it was provided to Outside Counsel, except to the extent that longer retention is required by applicable law, regulations, or professional ethical rules.

2.2 **Return/Destruction**

At the conclusion of the engagement and as instructed by Company, Outside Counsel shall (at its sole cost) return, delete, or destroy Company Confidential Information then in its possession or under its control including, without limitation, originals and copies of such Company Confidential Information. The following types of information are excluded from this requirement: (i) day-to-day exchanges of emails, except for those containing attachments that contain Company Confidential Information; (ii) Outside Counsel work product; (iii) Company Confidential Information that becomes a part of the public domain, including through court filings; and (iv) Company Confidential Information that Outside Counsel is required to maintain, by law, regulations, or professional ethical rules but for only the time period required. With respect to (i) herein, excluded emails should be handled consistently with Outside Counsel's professional duty of confidentiality. For the avoidance of doubt, anything that is stored on routine back-up media solely for the purpose of disaster recovery will be subject to destruction in due course rather than immediate return or destruction pursuant to this paragraph, provided that employees are precluded from accessing such information in the ordinary course of business prior to destruction. Notwithstanding the foregoing, latent data such as deleted files, and other non-logical data types, such as memory dumps, swap files temporary files, printer spool files, and metadata that can only be retrieved by computer forensics experts and is generally considered inaccessible without the use of specialized tools and techniques will not be within the requirement for return or destruction of Company Confidential Information as set forth by this provision.

2.3 **Certification**

Outside Counsel agrees to certify that Company Confidential Information has been returned, deleted, or destroyed from its systems, servers, off-site storage facilities, office locations, and any other location where Outside Counsel maintains Company Confidential Information within 30 days of receiving Company's request that the information be returned, deleted, or destroyed.

3. Data Handling

3.1 **Encryption**

3.1.1 **Encryption in Transit**

When transferring Company Confidential Information, and in communications between Company and Outside Counsel, Outside Counsel will use encryption based on guidance provided by Company, if any.

The Company reserves the right to request implementation of Transport Layer Security to automatically encrypt emails between Company and Outside Counsel.

Note: Section 3.1.2 below is highly recommended. Minimally, law firms should have mechanisms in place that provide for technologically equivalent mitigations in the absence of encryption at rest.

3.1.2 **Encryption at Rest**

Outside Counsel will encrypt all Company Confidential Information that resides on Outside Counsel's systems, servers, backup tapes, etc., including Company Confidential Information that resides on the systems and servers of any third party with which Outside Counsel has subcontracted to store electronic data. Outside Counsel shall encrypt at rest using solutions that are certified against U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and any keying material are not stored with any associated data.

3.1.3 **Encryption of Data Stored on Portable Devices or Transmitted Over Non-Secure Communication Channels**

Outside Counsel will encrypt all Company Confidential Information when stored on portable devices and media or when transmitted over non-secure communication channels (*e.g.*, internet email, or wireless transmission) including remote connectivity using solutions that are certified against the U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and any keying material are not stored with any associated data.

3.1.4 **Encryption of Company Confidential Information Transferrable to Removable Media and Mobile Devices**

In the event that Company Confidential Information could be transferred to removable

media, a mobile device, tablet, or laptop, Outside Counsel will implement, monitor, and maintain encryption and information leakage prevention tools using solutions that are certified against the U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated data. Moreover, two-factor authentication should be employed for remote connectivity using a mobile device, tablet, or laptop.

3.2 **Data Security Breach Reporting**

Upon discovering any suspected or actual unauthorized disclosure, loss, or theft of Company Confidential Information (a "Data Security Breach"), Outside Counsel will promptly (within 24 hours of discovering an actual or suspected event) send an e-mail to ***(insert email address of company contact***). Outside Counsel shall fully cooperate with Company to provide all information in a timely manner and shall fully cooperate with Company, as directed by Company, to make any notifications required by applicable law. Outside Counsel will fully cooperate with Company to identify a root cause and remediate any Data Security Breach at their sole cost. Outside Counsel shall designate an individual who will serve as Company's ongoing single point of contact for purposes of addressing issues with respect to the use and security of Company Confidential Information during the term and following the termination or expiration of these standards. Such individual shall be accessible to Company on a 24X7 basis. Outside Counsel shall certify that this individual can obtain relevant information specific to any incidents within 48 hours. This individual is to also have access to or direct knowledge of Outside Counsel's network architecture and information technology system.

3.3 **Compliance with Laws**

Outside Counsel will comply with all laws, regulations, statutes, and ordinances ("Laws") applicable to its business or the performance of its obligations pursuant to Company's engagement of Outside Counsel, as such Laws may be revised from time to time.

4. Physical Security

4.1 **General**

Company Confidential Information must be physically secured against unauthorized access.

Note: The Physical Security Protections in Section 4.2 are recommended for law firms that host Company Confidential Information on its systems and servers.

4.2 **Physical Security Protections**

Outside Counsel will implement at least the following:

1. Picture identification badges issued through Outside Counsel's formal approval processes.
2. Processes to remove leaver (*i.e.*, departing staff member) personnel from facility access within 24 hours of notification or within one hour in emergency/priority situations.
3. 24x7 security guards monitoring entrance(s) to the facility where Company Confidential Information is accessed, or comparable controls where Company Confidential Information is stored, processed, or destroyed.
4. Identity verification using government-issued IDs prior to entry to a facility where Company Confidential Information is accessed, stored, processed, or destroyed for all visitors, and visitors are supervised by a formal escort while on-site.
5. Electronic access control to any facility where Company Confidential Information is accessed, stored, processed, or destroyed using badge/access cards.
6. Enhanced access control for access to computer rooms within a facility that houses information systems hardware ("computer room") (*e.g.*, biometric safeguards such as palm readers, iris recognition, or fingerprint readers).
7. Camera surveillance (CCTV) with active monitoring or integration into a detection system.
8. A perimeter intruder alarm system (*e.g.,* open door alarms).
9. No exterior access points (*e.g.*, windows, exterior doors) are present within a computer room.
10. Backups are physically secured against unauthorized access.
11. Procedures are in place to verify that receiving/delivery of/removal of hardware and other equipment are authorized.
12. Physical access to facilities where Company Confidential Information is accessed, stored, processed, or destroyed must be logged. Logs must be retained for at least ninety days.

5. Logical Access Controls

Outside Counsel must have logical access controls designed to manage access to Company Confidential Information and system functionality on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, unique IDs and passwords, two-factor or stronger authentication for its employee remote access systems (and elsewhere where appropriate). These controls shall enable Outside Counsel to promptly revoke or change access in response to terminations or changes in job functions as applicable. Outside Counsel will encrypt all passwords, passphrases, and PINs using solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated data. Outside Counsel will implement any Company request to revoke or modify user access within twenty-four hours of receipt of Company's request. Outside Counsel will disable user accounts after at most 10 consecutive invalid authentication attempts.

6. Monitoring

Unless prohibited by applicable law, Company expects Outside Counsel to continuously monitor its networks and employees, subcontractors, and contingent workers for malicious activity and other activity that may cause damage or vulnerability to Company Confidential Information.

7. Vulnerability Controls and Risk Assessments

At least annually, Outside Counsel will perform vulnerability tests and assessments of all systems that contain Company Confidential Information. Outside Counsel must have application security software development controls designed to eliminate and minimize the introduction of security vulnerabilities. For any of Outside Counsel's applications that process Company Confidential Information, such testing must also include manual ethical hacking/penetration tests using intercept proxies to identify security vulnerabilities that cannot be discovered using automated tools, and code review or other manual verifications to occur at least annually or upon any major software change, including customizations for Company.

8. System Administration and Network Security

Outside Counsel must have operational procedures and controls designed to ensure that technology and information systems are configured and maintained according to prescribed internal standards and consistent with applicable Industry Standard Safeguards. Examples of Industry Standard Safeguards are ISO/IEC 27002:2005, NIST 800-44, Microsoft Security Hardening Guidelines, OWASP Guide to Building Secure Web Applications and the various Center for Internet Security Standards. Moreover, Outside Counsel must have application security and software development controls designed to eliminate and minimize the introduction of security vulnerabilities.

Antivirus protection shall be installed and configured to automatically search for and download updates (daily, at a minimum) and perform continuous virus scans. Malware and threat detection is to be updated continuously, and software patches provided by vendors shall be downloaded and implemented in a timely manner. If Outside Counsel is unable to implement these controls in a timely manner, Outside Counsel shall notify the Company in writing.

Outside Counsel shall have vulnerability management and regular application, operating system and other infrastructure patching procedures and technologies reasonably designed to identify, assess, mitigate, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

Outside Counsel shall have, shall implement, and shall maintain network security controls, including the use of firewalls, layered DMZs and updated intrusion, intrusion detection and prevention systems, reasonably designed to protect systems from intrusion or limit the scope or success of any attack or attempt at unauthorized access to Company Confidential Information.

9. Security Review Rights

Company and its agents, auditors (internal and external), regulators, and other representatives as Company may designate, may inspect, examine, and review the facilities, books, systems, records, data, practices, and procedures of Outside Counsel (and any subcontractors that Outside Counsel may use) that are used in rendering services to

Company to verify the integrity of Company Confidential Information and to monitor compliance with the confidentiality and security requirements for Company Confidential Information.

Note: Section 10 below is recommended but optional. ISO Certifications reduce the time and effort required by in-house IT security departments to perform security assessments on third parties in possession of Company Confidential Information.

10. Industry Certification/Additional Security Requirements

If Outside Counsel has not achieved ISO27001 certification, Company may request that Outside Counsel undertake the certification process and provide Company with evidence of certification when attained. Outside Counsel agrees to implement additional security requirements reasonably requested by Company, and provide Company with relevant additional information that Company may request such as SOC audits or other evidence that Outside Counsel has in place appropriate policies and procedures regarding information protection and security.

11. Background Screening of Outside Counsel Employees, Subcontractors, and Contingent Workers

Unless precluded by law or regulation, Outside Counsel agrees to conduct background screening for all of its employees, subcontractors, and contingent workers who work with or come into contact with Company Confidential Information. Outside Counsel will certify annually to Company that all of Outside Counsel's employees, subcontractors, and contingent workers that work with or come into contact with Company's Confidential Information have successfully passed Company's background screening requirements unless such background screening is precluded by law or regulation in a specific jurisdiction.

12. Cyber Liability Insurance

Without limiting its responsibilities set out in herein, in countries where cyber liability insurance coverage is available, Outside Counsel will obtain and maintain in force at all times cyber liability insurance with an insurance company having a minimum credit rating of A- from Standard and Poors or other equivalent rating agency, with a minimum coverage level of $10,000,000. All responsibility for payment of sums under any deductible or self-insured

retention provisions of the policy or policies remains with Outside Counsel. It is expressly understood and agreed that Company does not in any way represent that the above specified minimum coverage limit is sufficient or adequate to protect Outside Counsel's interests or liabilities. Outside Counsel shall name Company as an additional insured and provide a copy of its cyber-insurance certificate to Company upon written request.

13. Subcontractors

Outside Counsel shall be responsible for all subcontractors used by Outside Counsel that have access to Company Confidential Information. Where Outside Counsel subcontracts its obligations to Company to a third party, it shall do so only by way of written agreement imposing Company's *Model Information Protection and Security Controls for Law Firms Possessing Company Confidential Information* which pertains to all of Outside Counsel's subcontractors that possess or access Company Confidential Information. For the avoidance of doubt, this section pertains to, without limitation, reprographics vendors, off-site storage vendors, and cloud server hosting facilities.