Cybersecurity Policy

HANDBOOK

ACCELLIS
TECHNOLOGY GROUP

TABLE OF CONTENTS

Introduction

A law firm with four partners and a staff of ten is breached as part of an indiscriminate attack from a bot-net – a large group of computers infected with malicious software and controlled without the owners' knowledge – by 20-something year olds in Eastern Ukraine.

The vector of attack exploited outdated Adobe software on an attorney's laptop. The malicious code executed behind the firm's firewall and before encrypting all of their data to be ransomed back, the code scoured the network for personally identifiable data, such as social security numbers, dates of birth, and home addresses and copied it back to the hackers.

Within weeks, employees of the firm were well in the midst of dealing with identity theft to the tune of millions of dollars. And within three months, several of the staff filed suit against the partners for not doing enough to mitigate a cyber-attack or the resulting damages.

This is a scenario that is beginning to play out with greater frequency. For too long, firms have turned a blind eye to the growing threats to the cyber security of firm and client data. The attacks have grown more sophisticated than what a firewall and some anti-virus software on a desktop can handle.

The American Bar Association (ABA) has taken notice. To address the security needs of the legal industry, ABA Resolution 109 specifically recommends:

> ***That … all private and public sector organizations develop, implement, and maintain an appropriate security program, including:***
>
> *(1) conducting regular assessments of the threats, vulnerabilities, and risks to their data, applications, networks, and operating platforms, including those associated with operational control systems; and*
> *(2) implementing appropriate security controls to address the identified threats, vulnerabilities, and risks, consistent with the types of data and systems to be protected and the nature and scope of the organization*

Written security policies are the first step in demonstrating that your firm has taken reasonable steps to protect and mitigate the ever-growing threats to the firm's cyber security. This guide is intended to provide law firms with a list of the most urgent policies they need, why they are needed, and how to use them.

Based on the ISO 27001 standards for securing assets such as financial information, intellectual property, employee details or information entrusted to firms by third-parties, this handbook will outline where policies fall in the grand security scheme (which layer) and will outline the five categories of policies law firms need: overall security program and awareness, data handling, access to systems and sites, monitoring, and securing.

A Layered Approach to Cybersecurity

Layered security, or what is also known as 'Defense in Depth,' refers to the practice of combining multiple security controls to slow and eventually thwart a security attack. It's an approach recommended for law firms of nearly any size.

By combining a myriad of hardware, software, policy and assessment tools, a firm can significantly decrease its risk exposure. More simply, each attack vector at the firm is assailable, but those that are not part of a layered approach are most at risk. Let's begin by understanding the layers at hand.

1) Data - This is the sensitive information you house like SSNs, DOBS, financial records, merger & acquisition files, patents, trade secrets, contact lists and more.

   Relevant questions: Where is my data in space and time? On what specific drives? Utilizing what database technologies? Accessible remotely by what tools and people?

2) Application Security - These are the controls within your line-of-business applications like practice management, time and billing, accounting, document management, e-discovery, and so on.

   Relevant questions: Have we setup security profiles, access rights, permissions, ethical walls and passwords? Do we have or need dual-factor authentication? How are we sharing important documents and emails with clients?

3) IT Infrastructure Security - These are the actual hardware and software assets you employ for security like antivirus, antispam, firewall, content filtering, patch & vulnerability management, encryption, physical security and more.

   Relevant questions: Am I proactively managing security? Is the firewall fully employed or is it just on? Are we testing for new vulnerabilities on an ongoing basis? Do we have encryption for data at rest?

4) Education & Policy Enforcement - Refers to what we are here for today; the creation of firm policies and plans that constitute the firm's Cybersecurity Framework, such as written security policies, incident response plan, disaster recovery plan and more.

   Relevant questions: Are firm members trained on proper security? Do they know how to identify a malicious email or how to respond if they believe a virus has infected their PC? Are our policies adequate, written, updated and enforced?

5) Continual Assessment & Improvement - Finally, firms need an ongoing process for the testing of new attack vectors, the effectiveness of the CS Framework, and testing for weaknesses in the approach.

Relevant questions: Have new threats emerged? Do recent close-calls warrant a review of our practices? In spite of our efforts and security spend, are users really knowledgeable and therefore safe? Have any of the new programs or services we purchased this year compromised our security posture?

The purpose of this handbook is to assist firms with one of the imperatives within the Education & Policy Enforcement layer: the creation and use of policies. As mentioned, there are five categories of policies, which we will review now: overall security program and awareness, data handling, access to systems and sites, monitoring, and securing.

Overall Security Program & Awareness

The basis of any effective security program starts by defining the goals of the program, defining roles and responsibilities, establishing an incident response plan, and developing and conducting continual education to re-inforce the policies and controls.

A. Written Information Security Policy

A Written Information Security Policy (WISP) defines the overall security posture for the firm. It can be broad, if it refers to other security policy documents; or it can be incredibly detailed. Some firms find it easier to roll up all individual policies into one WISP. For example, you might find it easier to list out all of the policies for securing your firm's IT resources, such as passwords, mobile device management, email, etc. and simply write a paragraph of guidelines that firm member must follow.

The key components of a WISP include:

- Asset Inventory - This is an organizational evaluation of all informational assets the firm maintains including sensitive client and employee data
- Threat Assessment - This is an evaluation of what threats exists to those assets
- Disaster Recovery Plan – This is a technical plan that is developed for specific groups to allow them to recover a particular business application; ie, network share drives, practice management solutions, etc.
- Breach Notification Plan – This is a guideline for all critical parties if the firm's network is breached. It should include notification plans and contact information for authorities and client contacts and possibly credit monitoring services
- Security Awareness Plan – This is a training and management plan the outlines procedures for identifying unknown resources in the building, email security, required encryption, smart phone guidelines and safe Internet browsing.
- Guidelines for updating and testing the WISP on a regular basis

Real world use: Your city has an extended power outage, or your building burns down, or you suffer a data theft - what do you do? Who do you notify? Having a WISP means having a plan.

B. Roles & Responsibilities

In the event of a security incident, you simply will not have time to figure out who is responsible for what. If there is any hope in mitigating the damages related to a breach, swift action is paramount. The roles & responsibilities policy has one sole purpose – to outline who will approve the information security policy, assign security roles, coordinate and review the implementation of security across the organization.

The policy should define the make-up of the Security Team/Committee and should include a decision maker and a representative from the IT group. Responsibilities, such as those for internal control accountability, overview of systems management and prevention, and incident response should be assigned and written out.

Real world use: Cryptolocker encrypts all firm data, who notifies users to log out? Who contacts the IT department? Who contacts affected clients?

C. Incident Response and Security Event Plan

Having (and practicing) an incident response plan is probably one of the most crucial steps any organization can take. It is not a matter of *if* an incident will occur, it is *when* an incident will occur. Having a plan in place will significantly reduce the impact to the firm. A good and well-rehearsed plan will reduce the risk and exposure to the firm, clients, employees, and partners that may arise out of a data theft or data loss incident. Law firms have a duty to protect entrusted information and to properly respond to an incident.

The purpose of the security event plan is to define when an incident response plan is to be enacted. This policy is designed to reduce the exposure that may arise out of a data theft or data loss incident. The policy details the nature and scope of an incident and identifies what client information systems and types of personally identifiable information have been accessed or misused.

According to the American Bar Association, if you find that your confidential information has been breached or exposed, you are obligated to (Bro & Smedinghoff, 2014):

1. Investigate and remedy the problem
2. Notify persons whose personal information was compromised
3. Notify state enforcement agencies
4. Notify Credit Agencies

Most states expect these steps to be handled as quickly as possible. It is important to know that encrypted data represents a safe harbor from these rules. Also, specific rules can vary from state to state so be sure to research your responsibilities when creating your WISP.

A good plan will describe the necessary steps to be taken in the event of a computer emergency, network intrusion, and/or data loss – including identifying a security response team, procedures for responding to an event, identifying the point of the breach, mitigating damages, communication to firm members and clients, and when to involve law enforcement. One of the most important, but often skipped, parts of an incident response and security event plan are the schedules and procedures for testing the plan.

Real world use: Your servers experience drive failure and are out of warranty. You start the process of spinning an image in the Barracuda cloud and are back online. You operate several days this way before realizing you still haven't ordered the replacement hardware. Now you are several days behind the eight ball.

D. Security Awareness Training Policy

Education and enforcement is critical to the success of the firm's security program. All firm members should be well versed and fully comprehend the tools and policies in place to help protect sensitive firm data. The policy should enumerate all the necessary steps the firm will take to empower firm members, such as regularly scheduled security classes and white-hat testing to verify all the roles and responsibilities are fully understood.

Consider offering a mandatory security class, at least on a semi-annual basis. Establish a communications channel to provide updates to the information security policies and recent threats to firm members. As part of the security awareness training, conduct "pop quizzes" throughout the year to make sure users are following the proscribed policies.

Real world use: A firm wants new employees trained on proper security; what kind of security training will there be for practice management, time and billing, remote access, etc.? How does the firm intend to raise awareness of phishing and socially engineered attacks?

Data Handling

Data is at the heart of the matter when it comes to cybersecurity. Personal identifiable information (PII), client data – most of which is protected by attorney-client confidentiality, and financial information all represent what amounts to data gold. Policies and procedures that govern how data is handled – knowing how to classify data, how it is accesses, and the full life cycle of a record is essential.

A. Backup & Recovery Policy

The firm's data is only as good as its last test restore. The backup and recovery policy should describe in detail all the requirements and procedures for maintaining and recovering backup copies of private and confidential data. The policies should detail the schedules, media, and recovery procedures – including testing restoration of data on a regular basis.

The policy should detail what data is backed up, how it is backed up, where it is backed up to, and when it gets backed up. Two rules of thumb for backups: 1) Use a backup rotation such grandfather-father-son (GFS) or Tower of Hanoi in order to distribute the backups across a wide set of media, 2) Follow the 3-2-1 backup methodology which states there should be at least 3 copies of the data, on at least 2 different types of media, and at least 1 copy is stored offsite. The policy should also describe the test recovery procedure and schedule.

Real world use: A firm loses all their data; they go to their backups to find none are recoverable; now we're in real trouble. A proper backup plan includes periodic fire drills – that is, attempts to restore backup media to make sure backups are working.

B. Data Classification & Handling Policy

In efforts to minimize the unauthorized sharing of classified information, data handling and classification of that data set is required. Firm management would approve this information security policy, assign security roles and coordinate and review the implementation of security across the organization.

The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal and State law.

The policy should provide guidance of how data is classified and what level of dissemination is allowed. Typically, the policy contains a grid similar to the following:

Record Type	Restricted	Public
Client matter	X	
Blog article		X

Real world use: A firm has a policy of sending important information by encrypted email only; but what is considered 'important'?

C. Data Disposal & Data Retention Policy

This policy describes retention and destruction of physical and digital documents based on record-keeping requirements and practical business needs. This includes limiting data storage amount and retention time based on what is required for legal, regulatory, and business requirements; process for secure deletion of data when no longer needed; specific retention requirements for PII data; identifying and securely deleting stored sensitive data that exceeds defined retention requirements.

Take stock of the types of different records, where they are stored, and how much you have. For example, personnel records might be stored on paper in the file cabinet of the HR manager while financial and client data are all in electronic format. Each record type and how it is stored will have ramifications on how the record's life cycle will be managed. Different records in different forms require different periods of retention. There can be many types of records (HR, business, client, financial, etc.) and there are two forms (electronic and physical). Know the laws and regulations for certain types of records. The policy should define the rules that move records from online (production) to nearline (easily recoverable) to offline (offsite and archived).

Real world use: A firm replaces servers; the old servers are too old to keep; what should they do with the hardware? Where does it go? Should the drives be electromagnetically wiped?

Access to Systems

Firm members access data to create solutions for clients - this is the essence of practicing law. Policies that establish methodologies for accessing data and other critical systems need to be secure while allowing ample affordance to firm members.

A. Accounts Management Policy

Establishing the procedures for maintaining accounts and credentials to all systems is as basic as it gets. Accounts and user IDs must not be left available to users who no longer need access to firm systems. This policy defines the control requirements for the secure management of accounts on firm assets and communication systems.

When creating the policy, be sure to include standards for unique identification, such as a username. Define rules for account that have full control of information, such as system administrator accounts. Establish guidelines for account creation and removal.

Real world use: A firm wants to improve its security but has no policy for passwords. In absence of a policy, how will users manage password expiry, strength, rotation and multifactor authentication?

B. Acceptable Use Policy

Most firms have some sort of acceptable use policy already in place. This policy defines the activities that are permissible when using any firm assets, including but not limited to, computers, workstations, laptops, mobile devices, tablets, or any device that can communicate with firm systems. This applies to all users of firm information assets including but not limited to firm employees, partners, third-parties, interns, or guests of the firm. These rules of behavior apply to the use of firm-provided IT resources, regardless of the geographic location.

When writing an acceptable use policy, include guidelines that discuss how firm members should use company equipment, service such as email and Internet access, how they utilize social media, and appropriate responses.

Real world use: A firm wants to minimize socially engineered attacks but users are angry at losing social media access; is Reddit okay? What about Engadget? CNN?

C. Software Usage Policy

In most cases, firms do not own the software they are using. Typically, it is licensed from a variety of vendors and other sources, such as Microsoft. In order to guard against proliferation of data and software, the Software Usage policy defines the requirements for compliance with software license agreements and related copyrights on all firm computer and communications systems.

Along with detailing software licensing and usage restrictions, the policy should cover other areas of software management such as installations guidelines, procurement procedures, and support agreements.

Real world use: The software a firm has is expensive and powerful; it can do a lot; too much sometimes. What controls do you have in place to prevent users from circumventing security?

D. Systems Access Policy

The Systems Access Policy defines the requirements surrounding access to the all firm data and systems. The policy governs aspects of recording who accesses data and systems, when the access takes place, permissions to application and data, and other privileges granted by the firm.

Include policy statements that cover control to overall access to firm's systems. For example, specify access restrictions, user accountability, guidelines for controlling access, and system privileges. Be sure to include this policy as part of the overall security awareness training.

Real world use: There is no policy distinction between staff and partners in Worldox; both have access to all financial information. With a proper SAP roles are assigned to user groups to prevent staff from seeing (let alone unnecessarily searching through) information they do not have rights to.

E. Physical Security Policy

The Physical Security Policy should describe how the physical location is accessed, including all points on ingress and egress. If there is a video surveillance system, include the procedures for rotating times or video storage. Other times to consider when drafting the policy are equipment maintenance, cable security, environmental controls, intrusion protection, and facility structure.

Access to the physical offices or datacenters where the firm's IT infrastructure is housed should always be locked down.

Real world use: To maintain HIPAA compliance firms need a locked server room; if you work with hospitals and people have access to your server room like they do a national park, are you at risk?

F. Vendor Compliance Policy

Some of the more recent high-profile breaches did not occur by hacking through a corporate firewall. Instead, access to the internal networks were attained by a malicious actor posing as a third-party vendor to perform maintenance on site. This policy defines the requirements for establishing physical location and protection controls at firm facilities to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Your vendor policy should cover the general guidelines third-party vendors will follow as it pertains to protecting firm data. Managing the list of approved vendors, including regular re-authorizations, vendor access – both in physical and virtual contexts, and controlling access to as few firm recourses as necessary for the vendor to complete the job.

Real world use: Target was hacked by one of its repair contractors. Do your third-party party vendors and partners comply with basic Internet security practices?

Monitoring for Incidents

There is a plethora of activity on firm networks, some of which is benign, some is malicious. Firms require policies and procedures to constantly monitor activity and offer both preventive and detective controls.

A. System Management Policy

The Systems Management policy defines the requirements for managing defaults configurations and changes to firm applications, computers and communications systems. It should outline access restrictions, session controls, authorization controls, awareness training and vulnerability management.

This policy should include information statements on items such as single-function server, asset inventory, and baseline standards. Policy statements for managing the IT infrastructure should cover remote management, vulnerability scanning, patching and bug fixes and updating core systems and software.

Real world use: When does a suite like Amicus Attorney get upgraded – whenever you feel like it? When does it get patched – sooner? What is your plan for sudden data corruption? By managing these reactively you are wasting precious resources.

B. Monitoring Policy

As activity is logged, requirements for managing and monitoring the data that are generated by the firm's information technology infrastructure are defined in this policy – including planning, contents, retention and maintenance of log systems at the firm.

Monitoring policies need to identify the systems and controls that require event logging. Thresholds, once established, should be set so alerts and remediation can take place as soon as possible. Log maintenance and storage should be included as part of the backup and recovery plan and be available for the incident and security event plan.

Real world use: You provide employees with phones and an Exchange sync of client data; do you also have the authority to monitor GPS location? Perform a remote wipe? Decide and formalize this in a policy so when you need to do your job there is no ambiguity.

Securing Technology Resources

From mobile devices to social networking to the common desktop, firms use what can seem like a dizzying array of technological resources. As instrumental as those resources are to conducting business, each of them can serve as a vector of attack for hackers. Securing them through software and policy is a must.

A. Anti-Malware Policy

Malware is software written with malicious intent. Computer viruses, Trojan horses, worms, and spyware are examples of malware. The policy states the requirements for controls to prevent and detect the dissemination of any malicious software on firm computer and communications systems found on firm assets.

The anti-malware policy governs the centralized anti-malware system in place at the firm and should include guidelines for updates, rules for quarantining and/or removal, and communication efforts if malware is detected.

Real world use: Malware can be installed by clicking a link in a phishing email, or by clicking an ad that looks legitimate, or by other means. In order to effectively combat this attack vector, you will need to establish rules for using IT at the firm.

B. Clean Desk & Clear Screen Policy

Clean desks are the cornerstone of a secure workplace. In efforts to minimize the unauthorized sharing of classified information, clean desks are required. Guidelines are needed to accomplish clean desks and clear screens. Statements regarding screen locking and the use of post-it notes that contain sensitive information are a part of this policy.

C. Cloud Services

This policy applies to all external cloud services (e.g. cloud-based email, document storage, etc.). Personal accounts are excluded. This policy provides guidance for how to handle any services related to remote servers storing sensitive firm data.

The cloud services policy should layout the firm's position of non-managed cloud services, such as Gmail or DropBox. Expectations that work-related materials should not be transmitted over non-managed cloud services is a critical part of the policy.

Real world use: Many firms have consumer tools like Dropbox, Box, Drive and other cloud apps. Staff and partners alike may be unknowingly exposing your sensitive data. Having a policy forces everyone to uses industry best practices.

D. Email Policy

Email is the primary means of communication at the firm. Guidance is necessary for compliance reasons as well as congruity. This covers passwords for emails, acceptable use for emails, content restrictions, backup and monitoring.

Consider including policy statements as it relates to email that discuss acceptable content to be shared over email, email encryption, phishing and attachment handling.

Real world use: A firm wants to find all emails related to a case; they can perform a conflict check and export records, but wouldn't it be helpful if employees already had this information readily available? An email policy for retention can standardize the ways you save making finding what you need that much easier.

E. Encryption Policy

This policy defines the requirements for establishing the encryption implementation and management requirements related to the firm computer and communications systems infrastructure. By setting standards, the firm maintains the most relevant encryption technology is used.

Define places within the firm infrastructure where encryption is warranted, such as laptops, email, HR data, and other places where critical or otherwise sensitive data is stored.

Real world use: A firm has emphasized data encryption as an asset in its war against cyber criminals. But Sheila has no password on her phone where some of that data resides. Hackers log into her phone and bypass encryption. A policy ensures you can adequately defend against this attack vector.

F. Mobile Device Policy

Mobile devices are assets that the firm utilizes on an everyday basis. This policy determines the information security requirements for the protection of sensitive information while being transmitted or received over any type of mobile device.

A mobile device policy should detail how mobile devices are issued and managed. Password and access controls should also be defined. Mobile app installations guidelines and mobile device wiping and reset guidelines should also be included.

Any features of Mobile Device Management (MDM) plan should be documented: encryption, password expiry, content filtering, whitelisting, and more. Moreover, each class of data available to the device should be defined and policies around it enforced (i.e., Exchange sync, mobile app, emails, etc.).

Real world use: A firm has mobile devices with client, event, and task data. A phone is stolen and the attorney knows an important merger and acquisition document was present on the device. How can the data be removed?

G. Password Management Policy

Passwords are the primary token used to access firm information systems. How passwords should be handled must be properly coordinated and supported. Outlining specifics on how passwords should be managed by each employee is central to staying secure and compliant.

Password policies should describe how user passwords are created and managed. Include definitions on acceptable password characteristics such as password length, complexity, and a password-change schedule.

Real world use: A firm has one password to log on to Windows which enables password-free login to all applications and databases. The password hasn't been changed in three years. Worried yet? Maybe the password is 'password' – how about now?

H. Removable Media Policy

This policy defines the requirements for the proper handling of all media that contains firm information. In most organizations, information is generated and stored on many different types of media including paper documents, computer media, and a myriad of portable devices. Much of this information is considered confidential or sensitive, which requires that its handling is performed in a safe and secure manner.

The removable media policy should detail how the firm and firm member handle removable media such as USB drives and DVDs or CDs. Consider creating statements that restrict or control the use of USB thumb drives.

Real world use: A firm has prohibited using flash drives to store information of any kind, but has no media policy in place and therefore has implemented no security controls. This means the firm is relying on the honor system rather than using centralized management to disable the use of any media.

I. Social Media Policy

Social Media is a predominant part of popular culture and becoming an integral part of business. Firms use social media as means to advertise and keep in touch with clients. Firm policy statements on social media should protect the firm from the dissemination of sensitive information and/or damaging the firm's reputation.

Real world use: a firm encourages staff and attorneys to have a social media presence. A staff member happily announces to her 500 followers that the firm is helping merge two pharmaceutical companies. This sends one of the company's stock prices into a spiral and jeopardizes the deal; the company is talking about suing the firm for its market value loss.

J. Wireless Communication Policy

Firm members are constantly part of a connected world. This policy addresses the use of mobile communication devices via wireless communication either Wi-Fi internet or Bluetooth for business purposes – and methods for securing the communicated information.

This policy should describe how the firm protects its assets from unauthorized access over Wi-Fi and other wireless vectors. Statements should include the firm's position on personal hotspots and use of guest networks.

Real world use: Staff members are pressed for time so they decide to use Wi-Fi direct to transfer a document to an attorney. Problem is, the channel was poorly setup and the document is intercepted by opposing counsel just hours before trial.

Cybersecurity Policy Templates

A. Sample – Security Event Policy

See page 17

B. Sample - Social Media Policy

See page 29

C. Sample - Systems Management Policy

See page 33

Policy Title	Security Event Policy
Policy Number	ABC-123
Effective Date	INSERT DATE POLICY BECOMES ACTIVE
Responsible Office/Person	Security & Compliance Officer
Related Policies	ABC-321; ABC-456

I. Contents

II. BACKGROUND

The ABC Firm Security Event Policy has been developed to define when an incident response plan is to be enacted. This policy is designed to reduce the exposures to ABC Firm and the consumers, employees, and partners of ABC Firm that may arise out of a data theft or data loss incident. ABC Firm has an affirmative duty to protect consumer information and to properly respond to incidents. ABC Firm assesses the nature and scope of an incident, and identifies what client information systems and types of personally identifiable information have been accessed

or misused. ABC Firm will refer to ABC-321, Incident Response Plan to contain and control incidents to prevent further unauthorized access to, misuse of, consumer information, while preserving records and other evidence. Notifying appropriate law enforcement agencies will only happen if required by law.

III. SCOPE

This policy applies to the entire ABC Firm team, including the President, Director, employees, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with ABC Firm, as well as volunteers and guests who have access to ABC Firm assets. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by ABC Firm.

IV. DEFINITIONS

Policy – A policy is a governing set of principles that guide ABC Firm practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances the ABC Firm mission and values, and reduces organizational risks. It has broad application throughout ABC Firm. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

SRT **–** Security Response Team

V. COORDINATOR / POLICY AUTHOR

Security & Compliance Officer

VI. AUTHORIZING OFFICER

Director

VII. EFFECTIVE DATE

INSERT DATE POLICY BECOMES ACTIVE

VIII. REVIEW DATE

Annual Review

IX. POLICY STATEMENTS

Security Event Program Organization

Computer Emergency Response Plans - ABC Firm management must prepare, periodically update, and regularly review emergency response plans that provide for the continued

operation of critical computer and communication systems in the event of an interruption or degradation of service.

Incident Response Plan Contents - The ABC Firm incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise including notification of relevant external partners. Specific areas covered in the plan include:

- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Identification and coverage for all critical system components.
- Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers.

Annual Incident Response Testing - At least once every year, the Information Security Department must utilize simulated incidents to mobilize and test.

Security Response Team

Security Response Team - Information Technology Department management must organize and maintain an in-house security response team (SRT) that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related emergencies such as virus infestations and hacker break-ins. A member of the Information Security Department is notified of any emergencies or incidents.

Computer Incident Response Team Availability - The ABC Firm Computer Emergency Response Team must be available at all times to respond to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.

Testing The Computer Emergency Response Team - At least once per year, the Information Security Department must utilize simulated incidents to mobilize and test the adequacy of the ABC Firm Computer Emergency Response Team.

Roles and Responsibilities

Incident Management Responsibilities - The individuals responsible for handling information systems security incidents must be clearly defined by the Information Security Manager. These individuals must be given the authority to define the procedures and methodologies that will be used to handle specific security incidents.

Designated Contact Person for all disasters and Security Events - Unless expressly recognized as an authorized spokesperson for ABC Firm, no worker may speak with the press or any other outside parties about the current status of a disaster, an emergency, or a security event that has been recently experienced.

Providing Information In Legal Proceedings - Employees are prohibited from providing any ABC Firm records, or any copies thereof, to third parties outside of ABC Firm or to government officials, whether in answer to a subpoena or otherwise, unless the prior permission of the President has first been obtained. Likewise, employees are prohibited from testifying to facts coming to their knowledge while performing in their official ABC Firm capacities, unless the prior permission of the President has first been obtained.

Program Communication

Display of Incident Reporting Contact Information - ABC Firm contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters and the intranet.

Incident Response and Recovery

Intrusion Response Procedures – **ABC-016 Incident Response Plan** outlines the procedures for intrusion response. The Information Security Department must document and periodically revise intrusion response procedures to keep up with the changing technology. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

Information Security Problem Resolution - All information security problems must be handled with the involvement and cooperation of in-house information security staff, the ABC Firm Security Response Team, or others who have been authorized by ABC Firm.

Security Changes After System Compromise - Whenever a system has been compromised, or suspected of being compromised by an unauthorized party, System Administrators must immediately reload a trusted version of the operating system and all security-related software, and all recent changes to user and system privileges must be reviewed for unauthorized modifications.

Suspected System Intrusions - Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and predetermined procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

Unauthorized Access Problems - Whenever unauthorized system access is suspected or known to be occurring, ABC Firm personnel must take immediate action to terminate the access of

Internal Investigations Information Confidentiality - Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspected party.

Legal Proceeding Participation - Any ABC Firm worker called by a subpoena or in any other manner called to appear or testify before a judicial board or government agency must immediately notify the chief legal counsel in writing about the call.

Event Monitoring

Monitoring Event Logs - The usage of all ABC Firm shared computing resources employed for production activities must be continuously monitored and recorded. This usage history data must in turn be provided in real-time to those security alert systems designated by the Information Security Department (intrusion detection systems, virus detection systems, spam detection systems, etc.). When possible, all event logs will be shipped to a central logging system setup and retained per the **ABC-456 Disposal & Data Retention Policy**.

Intrusion Detection Systems - On all internal servers containing sensitive data, ABC Firm must establish and operate application system logs, intrusion detection systems, and other unauthorized activity detection mechanisms specified by the Information Security Department.

Reporting Information Security Events

Incident Reporting - All suspected information security incidents must be reported as quickly as possible through the approved ABC Firm internal channels.

Information Security Alert System - All ABC Firm employees are required to immediately inform the Information Security Department regarding any suspected information security problems.

Violation And Problem Reporting Protection - ABC Firm will protect employees who report in good faith what they believe to be a violation of laws or regulations, or conditions that could jeopardize the health or safety of other employees. Employees will not be terminated, threatened, or discriminated against because they report what they perceive to be a wrongdoing or dangerous situation.

Violation And Problem Reporting Identity Protection - Employees who report to the Information Security Department a security problem, vulnerability, or an unethical condition within ABC Firm may, at their discretion, have their identity held in strict confidence. This means that the whistleblower's immediate supervisor, other members of the management team, as well as other ABC Firm employees who are not directly involved in the receipt of the report, will not be given the whistleblower's identity.

Events to Report

Off-Site Systems Damage And Loss - Employees must promptly report to their manager any damage to or loss of ABC Firm computer hardware, software, or information that has been entrusted to their care.

System Alerts and Warnings - Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Security Department. Users are prohibited from utilizing ABC Firm systems to forward such information to other users, whether the other users are internal or external to ABC Firm.

Unauthorized Activity - Users of ABC Firm information systems must immediately report to the Information Security Manager any unauthorized loss of, or changes to computerized production data. Any questionable usage of files, databases, or communications networks must likewise be immediately reported.

Unexpected Requests For Log-In Information - Other than the regular and expected ABC Firm log-in screens, users must be suspicious of all pop-up windows, web sites, instant messages, and other requests for a ABC Firm user ID and password. Users encountering these requests must refrain from providing their ABC Firm user ID and password, as well as promptly report the circumstances to the Help Desk.

Missing Access Devices - Identification badges and physical access cards that have been lost or stolen--or are suspected of being lost or stolen--must be reported to the Information Security Department immediately. Likewise, all computer or communication system access tokens (smart cards with dynamic passwords, telephone credit cards, etc.) that have been lost or stolen--or are suspected of being lost or stolen--must be reported immediately.

Unintended Sensitive Information Disclosures - Unintended disclosures of sensitive ABC Firm information are serious matters, and they must all be immediately reported to both the Director of Client Services and the Information Security Manager. Such reporting must take place whenever such a disclosure is known to have taken place, or whenever there is a reasonable basis to believe that such a disclosure has taken place.

Software Malfunctions - All apparent software malfunctions must be immediately reported to the Information Security Manager. Security manager will document the malfunction with Connect-wise and contact the Director of Client Services.

Unauthorized Wireless Access Points - If an unauthorized wireless access point is detected on the ABC Firm network the Information Security Department must be notified.

Reporting to Third Parties

External Violation Reporting - Unless required by law or regulation to report information security violations to external authorities, management, in conjunction with representatives from the Information Security Department must weigh the pros and cons of external disclosure before reporting these violations.

Reporting Suspected Security Breaches To Third Parties - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

Loss Or Disclosure Of Sensitive Information - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Information Security Department must be notified immediately.

System Vulnerability Exploitation And Victim Data - ABC Firm staff must not publicly disclose information about the individuals, organizations, or specific systems that have been damaged by computer crimes and computer abuses. Likewise, the specific methods used to exploit certain system vulnerabilities must not be disclosed publicly.

Vendor Vulnerability Disclosure - If a serious information system vulnerability is discovered by ABC Firm employees, and the vulnerability can be directly traced to a weakness in a certain vendor's hardware and/or software, then that vendor must promptly and confidentially be notified of the problem.

Contact with Authorities

Criminal Justice Community Contact - Technical information systems staff must not contact the police or other members of the criminal justice community about any information systems problems unless they have received permission from the Chief Executive Officer.

Law Enforcement Inquiries - Even if the requesting party alleges to be a member of the law enforcement community, ABC Firm employees must not reveal any internal ABC Firm information through any communications mechanism unless they have established the authenticity of the individual's identity and the legitimacy of the inquiry.

Contacting Law Enforcement - Every decision about the involvement of law enforcement with information security incidents or problems must be made by an ABC Firm senior partner. Likewise, every contact informing law enforcement about an information security incident or problem must be initiated by the Information Security Manager.

Requests To Cooperate In Investigations - ABC Firm employees must immediately report every request to participate in an information security investigation to the Chief Executive Officer. Any sort of cooperation with the requesting party is prohibited until such time that the President has determined that the participation is legal, is unlikely to cause problems for ABC Firm, and is requested by an authorized party.

Data Breach Management

Data Breach Response Plan Required - ABC Firm management must prepare, regularly review, and update a Data Breach Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

Incident Review

Incident Response Plan Evolution - Lessons Learned - The incident response plan must be updated to reflect the lessons learned from actual incidents and developments in the industry.

Violation And Problem Analysis - An annual analysis of reported information security problems and violations must be prepared by the Information Security Department.

Collection of Evidence

Computer Crime Or Abuse Evidence - To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. The information to be immediately collected includes the current system configuration, all related event logs, as well as backup copies of all potentially involved files.

Evidence Storage -The relevant information for computer investigation must then be securely stored off-line until official custody is given to another authorized person or the President determines that ABC Firm will no longer need the information.

Sources Of Digital Evidence - For every production computer system, the Information Security Department must identify the sources of digital evidence that reasonably could be expected to be used in a court case. These sources of evidence must then be subject a standardized capture, retention, and destruction process comparable to that used for vital records.

Responsibility for Electronic Evidence Production - ABC Firm will appoint a single individual responsible for coordinating the discovery and presentation of electronic evidence that may be required to support litigation.

Information Classification - ABC Firm data that may be considered electronic evidence must be classified as CONFIDENTIAL and viewed only by authorized representatives or approved third parties involved in the investigation.

Investigation and Forensics

Computer Crime Investigation - Whenever evidence clearly shows that ABC Firm has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

Extended Investigations - Extended investigations of security breaches must be performed while the suspected worker is given leave without pay. The reason for a suspect's leave without pay must not be disclosed to co-employees without the express permission of the President.

Forensic Analysis Data Protection - Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.

Investigation Status Reports - The status of information security investigations must be communicated to management only by the lead investigator or the management representative of the investigation team.

Computer Crime Investigation Information - All evidence, ideas, and hypotheses about computer crimes experienced by ABC Firm, including possible attack methods and perpetrator intentions, must be communicated to the President and treated as restricted and legally privileged information.

Information Security Investigations - All ABC Firm internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the Information Security Manager.

Information Security Investigation Teams - Any person who personally knows the suspects, or who is friendly with them, for conflict of interest reasons is barred from participating on an information security incident investigation team.

Intrusion Investigations Details - Details about investigations of information system intrusions that may be still underway must not be sent via electronic mail. Likewise, to prevent such information from falling into the hands of intruders, files which describe an investigation now underway must not be stored on potentially compromised systems or anywhere on a related network where they could be reasonably expected to be viewed by intruders.

X. EXCEPTIONS

Exceptions to this policy will only be allowed with documentation and Director written approval. If any exception must be made, Director must approve.

XI. VIOLATIONS

Violations will be met with verbal or written acknowledgement of the violation. Director will determine if further action is to be taken.

Approved: _____ Date: _____

(Sam Smith)
(CEO)

XII. Document History			
Version	Date	Author	Comments
V1	5/13/2015	Mary Smith	Document Creation
V2	5/20/2015	Joe Johnson	Personnel Labels
V3	6/17/2015	Fred Roberts	Proof

Policy Title	Social Media Policy
Policy Number	ABC-567
Effective Date	INSERT DATE POLICY BECOMES ACTIVE
Responsible Office/Person	Security & Compliance Officer
Related Policies	ABC-001; ABC-006; ABC-022; ABC-011;

I. Contents

II. BACKGROUND

Social Media is a predominant part of popular culture. ABC Firm uses social media as means to advertise. How users act in an online manner is sensitive and this policy outlines policies that best reflect ABC Firm.

III. SCOPE

This policy applies to the entire ABC Firm team, including the President, Director, employees,

temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with ABC Firm, as well as volunteers and guests who have access to ABC Firm assets. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by ABC Firm.

IV. DEFINITIONS

Policy – A policy is a governing set of principles that guide ABC Firm practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances the ABC Firm mission and values, and reduces organizational risks. It has broad application throughout ABC Firm. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

V. COORDINATOR / POLICY AUTHOR

Security & Compliance Officer

VI. AUTHORIZING OFFICER

Director

VII. EFFECTIVE DATE

(Determined by Director)

VIII. REVIEW DATE

Annual Review

IX. POLICY STATEMENTS

Company Assets - ABC Firm recognizes that employees may have personal accounts on Facebook, Linked-In, Twitter, Web-based email accounts such as Gmail, Hotmail and Yahoo. ABC Firm understands that employees may want to review those accounts during work days utilizing the company's electronic assets. It is approved to use social media on company assets only if necessary for company use.

Personal use - of social media should be reserved for break times and meal periods.

Social Media Privacy - ABC Firm users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to social media, this includes passwords, codes or other information that is entered on any company asset. **ABC-006 Acceptable Use Policy, ABC-022 Monitoring Policy,** and **ABC-011 Data Classification & Handling Policy** all outline strict rules for monitoring all data in and out of the network; this applies to all social media accessed from inside ABC Firm systems.

Social Media Slander - If you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or suppliers, or that might constitute harassment or bullying. ABC Firm expects all users to act in a morally exemplary manner wherever they may express themselves. Examples of in-appropriate conduct include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

Sensitive Information on Social Media - Maintain the confidentiality of ABC Firm trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications on any social media or any other system not approved by the Security Department.

Company Opinions - Express only your personal opinions. Never represent yourself as a spokesperson for ABC Firm.

Social Media Advertising - ABC Firm may develop social media accounts for advertising purposes. Users may be asked to contribute to or maintain these accounts on behalf of the company. Only approved content may be posted to these social media accounts and the accounts may only be used for business purposes. The accounts, logins, passwords, information found on the accounts and any posts and/or submissions are the property of ABC Firm.

X. EXCEPTIONS

Exceptions to this policy will only be allowed with documentation and Director written approval.

XI. VIOLATIONS

Violations will be met with verbal or written acknowledgement of the violation. Director will determine if further action is to be taken.

Approved: _____ Date: _____
(Sam Smith)
(CEO)

XII. DOCUMENT HISTORY			
Version	Date	Author	Comments
V1	5/18/2015	Joe Smith	Document Creation
V2	5/22/2015	Fred Roberts	Personnel Labels
V3	6/17/2015	Sally Johnson	Proof

Policy Title	System Management Policy
Policy Number	ABC-789
Effective Date	INSERT DATE POLICY BECOMES ACTIVE
Responsible Office/Person	Security & Compliance Officer
Related Policies	ABC-987; ABC-456;

I. Contents

II. BACKGROUND

This policy defines the requirements for managing defaults configurations and changes to ABC Firm application, computer, and communications systems. This policy outlines access restrictions, session controls, authorization controls, awareness training, and vulnerability management.

III. SCOPE

This policy applies to the entire ABC Firm team, including the President, Director, employees, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with ABC Firm, as well as volunteers and guests who have access to ABC Firm assets. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by ABC Firm.

IV. DEFINITIONS

Policy – A policy is a governing set of principles that guide ABC Firm practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances the ABC Firm mission and values, and reduces organizational risks. It has broad application throughout ABC Firm. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

V. COORDINATOR / POLICY AUTHOR

Security & Compliance Officer

VI. AUTHORIZING OFFICER

Director

VII. EFFECTIVE DATE

INSERT DATE POLICY BECOMES ACTIVE

VIII. REVIEW DATE

Annual Review

IX. POLICY STATEMENTS

Authorization

Production Operation Access Controls - All user-level and administrative-level access controls required by ABC Firm information security policies must be established and enabled before production information systems can be placed into operation.

Single Function Servers – Whenever possible, critical production servers should limit functionality to only one core network service (electronic mail, database server, web server, etc.). This will ensure down time is minimized.

Component Inventory – ABC Firm must maintain an inventory of all systems and related components that are under the scope of each system.

Configuration Controls

Baseline Standards – All information systems placed into product must conform to minimum security configurations standards defined by the Security Department.

Default Passwords - All vendor-supplied default passwords must be changed before any computer or communications system is used for ABC Firm business.

User ID Review - Before any production multi-user computer operating system is installed at ABC Firm, all privileged user IDs that are not assigned to a specific employee or partner must be renamed or disabled.

Unnecessary Software - Software features that could be used to compromise security, and that are clearly unnecessary in the ABC Firm computing environment, must be disabled at the time when software is installed on multi-user systems.

Unnecessary Functionality - All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers, must be removed from the ABC Firm computer and communication infrastructure.

Remote Management

Access Encryption – All non-local access to ABC Firm systems must be encrypted using methods approved by the Security Department. All web-based access must use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Local Administration For Critical Systems – All ABC Firm critical product systems must be configured to only allow local administration.

Patches and Updates

Systems Administrators Install/Update Server Software - Only authorized Systems Administrators are permitted to install and/or update software on ABC Firm servers. See **ABC-987 Roles and Responsibilities Policy** for more instructions on who has access.

Software Patches, Bug Fixes, And Upgrades - All ABC Firm networked production systems must have an adequately-staffed process for expediently and regularly reviewing and installing all newly released systems software patches, bug fixes, and upgrades.

Security Patch Installation - All ABC Firm computer and communications system components and software must have the latest vendor-supplied security patches installed.

Critical Security Patch Installation Timing - All critical new security patches must be installed on ABC Firm computer and communications systems within one week.

Non-Critical Security Patch Installation, Fixes, And Upgrades - All non-critical security patches must be installed on ABC Firm computer and communications systems within one month.

Documenting Reasons Why Patches And Fixes Were Not Installed - If a patch or fix is not installed due to application conflicts or other incompatibilities, the involved Systems Administrator must document the reason and forward the documentation to the Security Department. These unpatched or unfixed vulnerabilities must be addressed and resolved to the satisfaction of the Security Manager during the next weekly information security review.

Third Party Applications - Executable programs provided by third party entities must be tested in accordance with Company policies and must also be properly documented before installation on any ABC Firm production system.

Vulnerability Management

Vulnerability Advisories - On a weekly or more frequent basis, the Security Department must review all information security vulnerability advisories issued by trusted organizations for items affecting ABC Firm systems.

Vulnerability Identification Software - To ensure that ABC Firm technical staff has taken appropriate preventive measures, all systems directly-connected to the Internet must be subjected to an automated risk analysis performed via vulnerability identification software at least once a month.

External Vulnerability Scans – Scan software to check all external facing vulnerabilities will be ran on ABC Firm systems once per month.

Internal Vulnerability Scans – Scan software to check all internal facing vulnerabilities will be ran on ABC Firm systems once per quarter or every 90 days.

Security Special Interest Groups - ABC Firm information security professionals must maintain memberships with security forums and professional associations to receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities.

System Security Status Tools - Every multi-user system must include sufficient automated tools to assist the Security Administrator in verifying the security status of the computer and must include mechanisms for the correction of security problems.

X. EXCEPTIONS

Exceptions to this policy will only be allowed with documentation and Director written approval.

XI. VIOLATIONS

Violations will be met with verbal or written acknowledgement of the violation. Director will determine if further action is to be taken.

Approved: _____ Date: _____

(Sam Smith)

(CEO)

XII. DOCUMENT HISTORY

Version	Date	Author	Comments
V1	5/18/2015	Mary Johnson	Document Creation
V2	5/22/2015	John Smith	Personnel Labels
V3	6/17/2015	Bob Roberts	Proof

Accellis Technology Group

Accellis Technology Group is one of the nation's leading providers of IT Consulting & Managed Services for the legal industry. We help law firms of all sizes reduce their day-to-day administrative tasks so they can focus on growing their business. Whether you need quicker access to help desk support, proactive IT management, improved security, or custom software solutions, Accellis can provide the expertise and direction to meet your goals.

This guide was developed by Accellis Technology Group based on years of field experience in the legal industry and is based on the ISO 27001 standards. Accellis Technology Group provides no warranties with respect to the guidance provided by this tool. Businesses should consult a cybersecurity expert before implementing any of the recommendations in this guide.

Additional resources:

- Law Firm Cyber Security Threat Matrix
- Avoid These Three Common Security Blind Spots
- Penetration Testing vs. Vulnerability Scanning
- Law Firm Cybersecurity: Practical Tips for Protecting Your Data
- Which type of hackers represent the biggest threat to law firms?
- The Biggest Cyber Security Threat to Law Firms is Not What You Think

Schedule a Free Consultation.

Accellis Technology Group helps simplify and streamline your cybersecurity and compliance efforts. We help you get in front of potential threats by ensuring your systems and policies are up-to-date with the today's latest industry standards and expectations.

Whether it's a security assessment, penetration test, or compliance evaluation – our team of certified security experts can ensure you're on the right track.

Schedule a Consultation

ACCELLIS
TECHNOLOGY GROUP