

# Information Security Policy

**RightCapital Inc.**

Last revision date: 2/6/2025

Document owner: Shuang Chen

<b><u>1</u></b>	<b><u>INTRODUCTION</u></b>	<b><u>4</u></b>
1.1	PURPOSE	4
1.2	SCOPE	4
1.3	ACRONYMS / DEFINITIONS	4
<b><u>2</u></b>	<b><u>EMPLOYEE RESPONSIBILITIES</u></b>	<b><u>6</u></b>
2.1	EMPLOYEE REQUIREMENTS	6
2.2	PROHIBITED ACTIVITIES	6
2.3	ELECTRONIC COMMUNICATION, E-MAIL, INTERNET USAGE	7
2.4	REPORT SECURITY INCIDENTS	8
<b><u>3</u></b>	<b><u>IDENTIFICATION AND AUTHENTICATION</u></b>	<b><u>9</u></b>
3.1	USER LOGON IDS	9
3.2	PASSWORDS	9
3.3	CONFIDENTIALITY AGREEMENT	9
3.4	ACCESS CONTROL	9
3.5	USER LOGIN ENTITLEMENT REVIEWS	9
3.6	TERMINATION OF USER LOGON ACCOUNT	9
<b><u>4</u></b>	<b><u>NETWORK SECURITY</u></b>	<b><u>10</u></b>
4.1	FIREWALLS	10
4.2	DDOS MITIGATION	10
4.3	SPOOFING AND SNIFFING PROTECTIONS	10
4.4	PORT SCANNING	10
4.5	WIRELESS ACCESS POINT AND NETWORKS	10
4.6	VULNERABILITY AND PENETRATION TESTING	10
<b><u>5</u></b>	<b><u>MALICIOUS CODE</u></b>	<b><u>12</u></b>
5.1	ANTIVIRUS SOFTWARE INSTALLATION	12
5.2	NEW SOFTWARE DISTRIBUTION	12
<b><u>6</u></b>	<b><u>ENCRYPTION</u></b>	<b><u>13</u></b>
6.1	DEFINITION	13
6.2	ENCRYPTION KEY	13
6.3	DATA IN TRANSIT	13

6.4	DATA AT REST	13
<b>7</b>	<b>DATA SECURITY, PROTECTION, BACKUP, RECOVERY</b>	<b>14</b>
7.1	DATA CENTERS	14
7.2	DATA SECURITY	14
7.3	PAYMENT PROCESSING	14
7.4	BACKUPS	14
7.5	DISASTER RECOVERY	14
<b>8</b>	<b>SPECIFIC PROTOCOLS AND DEVICES</b>	<b>14</b>
8.1	WIRELESS USAGE STANDARDS AND POLICY	14
8.2	USE OF TRANSPORTABLE MEDIA	15
8.3	OTHER PROHIBITIONS ON SENSITIVE DATA	15
<b>9</b>	<b>DISPOSAL OF PAPER AND/OR REMOVABLE MEDIA</b>	<b>16</b>
9.1	DISPOSAL OF PAPER	16
9.2	DISPOSAL OF REMOVABLE MEDIA	16
9.3	REQUIREMENTS REGARDING EQUIPMENT	16
9.4	DISPOSITION OF EXCESS EQUIPMENT	16
<b>10</b>	<b>CHANGE MANAGEMENT</b>	<b>17</b>
<b>11</b>	<b>AUDIT CONTROLS</b>	<b>18</b>
<b>12</b>	<b>INFORMATION SYSTEM ACTIVITY REVIEW</b>	<b>19</b>
<b>13</b>	<b>BUSINESS CONTINUATION PLAN</b>	<b>21</b>
<b>14</b>	<b>SECURITY AWARENESS AND TRAINING</b>	<b>23</b>
<b>15</b>	<b>SECURITY MANAGEMENT PROCESS</b>	<b>25</b>
<b>16</b>	<b>EMPLOYEE BACKGROUND CHECKS</b>	<b>28</b>
<b>17</b>	<b>BREACH NOTIFICATION PROCEDURES</b>	<b>30</b>
<b>19</b>	<b>POLICY GOVERNANCE</b>	<b>32</b>

# 1 Introduction

---

## 1.1 PURPOSE

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at RightCapital, hereinafter, referred to as the **Company**. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Company with policies and guidelines concerning the acceptable use of Company technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Company employees or temporary workers at all locations and by contractors working with the Company as subcontractors.

## 1.2 SCOPE

This policy document defines common security requirements for all Company personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Company, entities in the private sector, in cases where a Company has a legal, contractual or fiduciary duty to protect said resources while in Company custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Company network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Company in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Company domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Company at its office locations or at remote locales.

## 1.3 ACRONYMS / DEFINITIONS

Common terms and acronyms that may be used throughout this document.

**CEO** – The Chief Executive Officer is responsible for the overall privacy and security practices of the company.

**CIO** – The Chief Information Officer

**Encryption** – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific ‘need to know.’

**External Media** –i.e., CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

**FAT** – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

**Firewall** – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

**FTP** – File Transfer Protocol

**IT** - Information Technology

**LAN** – Local Area Network – a computer network that covers a small geographic area, i.e., a group of buildings, an office.

**NTFS** – New Technology File Systems – NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

**SOW - Statement of Work** - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

**User** - Any person authorized to access an information resource.

**Privileged Users** – system administrators and others specifically identified and authorized by Company management.

**Users with edit/update capabilities** – individuals who are permitted, based on job assignment, to add, delete, or change records in a database.

**Users with inquiry (read only) capabilities** – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

**VLAN** – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

**VPN** – Virtual Private Network – Provides a secure passage through the public Internet.

**WAN** – Wide Area Network – A computer network that enables communication across a broad area, i.e., regional, national.

**Virus** - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

## 2 Employee Responsibilities

---

### 2.1 EMPLOYEE REQUIREMENTS

The first line of defense in data security is the individual employee. Employees are responsible for the security of all data which may come to them in whatever format. The Company is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear an Identifying Badge so that it may be easily viewed by others - In order to help maintain building security, all employees should prominently display their employee identification badge.

Challenge Unrecognized Personnel - It is the responsibility of all company personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted company office location, you should challenge them as to their right to be there. All visitors to company offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the company. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Company policy states that all computers will have the automatic screen lock function set to automatically activate upon 15 minutes of inactivity. Employees are not allowed to take any action which would override this setting.

### 2.2 PROHIBITED ACTIVITIES

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.  
Exception: Authorized information system support personnel, or others authorized by the Company Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Company computers must be approved by the Company.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Company is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Company is strictly prohibited.
- Removable media use: Use of removable media is prohibited.

## 2.3 ELECTRONIC COMMUNICATION, E-MAIL, INTERNET USAGE

As a productivity enhancement tool, the Company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Company owned equipment are considered the property of the Company – not the property of individual users. Consequently, this policy applies to all Company employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Company provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

- 1) it does not consume more than a trivial amount of employee time or resources,
- 2) it does not interfere with staff productivity,
- 3) it does not preempt any business activity,
- 4) it does not violate any of the following:
  - a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
  - b) Illegal activities – Use of Company information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
  - c) Commercial use – Use of Company information resources for personal or commercial profit is strictly prohibited.
  - d) Political Activities – All political activities are strictly prohibited on Company premises. The Company encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.
  - e) Harassment – The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Company prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
  - f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.
  - g) Proprietary information – Any confidential, proprietary, or sensitive information belonging to or regarding employees, customers, or partners of RightCapital may not be transmitted.

Generally, while it is **NOT** the policy of the Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the Company’s equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers

dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Company reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Company policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

## **2.4 REPORT SECURITY INCIDENTS**

It is the responsibility of each Company employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer. Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Company CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Company CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Company Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.



## 3 Identification and Authentication

---

### 3.1 USER LOGON IDS

Individual users shall have unique logon IDs and passwords. Access Control Policy includes all the details regarding User Logon IDs.

### 3.2 PASSWORDS

#### **User Account Passwords**

User IDs and passwords are required in order to gain access to all Company networks and workstations. Access Control Policy includes all the details regarding Passwords.

### 3.3 CONFIDENTIALITY AGREEMENT

Users of Company information resources shall sign, as a condition for employment, an appropriate confidentiality agreement.

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign the Employee Non-Disclosure Agreement document prior to accessing Company information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending, or employees are leaving an organization.

### 3.4 ACCESS CONTROL

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e., port protection devices, firewalls, host-based authentication, etc.). Detailed Access control policies are included in the Access Control Policy Document.

### 3.5 USER LOGIN ENTITLEMENT REVIEWS

User Login entitlement is reviewed on a regular basis. Detailed Access control policies are included in the Access Control Policy Document.

### 3.6 TERMINATION OF USER LOGON ACCOUNT

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department by submitting the Request to Offboard the employee via internal ticketing system. Detailed Termination of User process is included in the Access Control Policy Document.

## 4 Network Security

---

### 4.1 FIREWALLS

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

### 4.2 DDOS MITIGATION

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

### 4.3 SPOOFING AND SNIFFING PROTECTIONS

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. RightCapital utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

### 4.4 PORT SCANNING

Port scanning is prohibited, and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped, and access is blocked.

### 4.5 WIRELESS ACCESS POINT AND NETWORKS

Wireless access point does not broadcast its Service Set Identifier (SSID). WiFi Protected Access 2 (WPA-2) encryption is used for data being transmitted between employee's computers and the wireless access point.

### 4.6 VULNERABILITY AND PENETRATION TESTING

On at least an annual basis, RightCapital will perform or engage a third party to perform a vulnerability assessment and penetration testing to ensure that the network is safe, secure, and the risk of external attack is mitigated.

## 5 Malicious Code

---

### 5.1 ANTIVIRUS SOFTWARE INSTALLATION

RightCapital platform servers housed at AWS and are Linux based. Highly controlled Linux based servers are not equipped with antivirus or malware protection tools.

RightCapital employees are supplied with Apple MacBook devices, guaranteeing built-in virus protection via XProtect and increased resilience to malware.

### 5.2 NEW SOFTWARE DISTRIBUTION

Only software created by Company application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. All new software will be tested by appropriate personnel in order to ensure compatibility with the currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from the Internet.

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Company computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Company hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

# 6 Encryption

---

## 6.1 DEFINITION

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is called cipher text.

## 6.2 ENCRYPTION KEY

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In conflict, the Company shall establish the criteria with the Privacy Officer or appropriate personnel. The Company employs several methods of secure data transmission.

## 6.3 DATA IN TRANSIT

All data transmission between employee computers and cloud servers must be encrypted.

Only encryption algorithms from NSA Suite B Cryptography can be used, unless approved by CTO.

## 6.4 DATA AT REST

All client information must be encrypted when stored in the cloud. The documents must be encrypted with Advanced Encryption Standard 256.

All employee computer hard drives should use full disk encryption (FDE).

Approved FDE are:

- FileVault 2 on Mac
- Bitlocker on Windows

## 7 Data Security, Protection, Backup, Recovery

---

### 7.1 DATA CENTERS

All business files and client information must be stored in approved data center facilities.

Approved data centers are:

- AWS North Virginia region
- AWS Ohio region
- AWS Oregon region
- AWS North California region

### 7.2 DATA SECURITY

Security monitoring must be in place for all servers and data centers. Full vulnerability scans of all environments hosting client data must be completed no less frequently than each calendar quarter.

### 7.3 PAYMENT PROCESSING

All client payments must be processed by a PCI compliant payment processor.

### 7.4 BACKUPS

All customer data must be backed up at least daily. At least backups of the most recent 30 days must be maintained.

### 7.5 DISASTER RECOVERY

All customer data must be maintained in at least two different physical locations.

## 8 Specific Protocols and Devices

---

### 8.1 WIRELESS USAGE STANDARDS AND POLICY

Due to the emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Company employees. This policy outlines the processes and

procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Company laptops and mobile devices.

Software Requirements - The following is a list of minimum software requirements for any Company laptop that is granted the privilege to use wireless access:

- Mac OS 10.13 High Sierra or later
- Windows 10 or later + Company approved antivirus software
- Full Disk Encryption
- Appropriate VPN Client, if applicable

## **8.2 USE OF TRANSPORTABLE MEDIA**

Company laptops

The Company utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Company laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

## **8.3 OTHER PROHIBITIONS ON SENSITIVE DATA**

In addition to the above, sensitive data may not be shared outside of RightCapital via any mechanism, including but not limited to e-mail or other electronic communication, bulletin boards, social media platforms, or forums.

Sensitive data related to RightCapital partners or customers cannot be bulk exported from RightCapital software, and RightCapital will not develop any functionality to allow for such export of sensitive data.

## 9 Disposal of Paper and/or Removable media

---

### 9.1 DISPOSAL OF PAPER

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Company work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: No removable media is allowed. Company laptops are wiped clean of all data when decommissioned.

### 9.2 DISPOSAL OF REMOVABLE MEDIA

No removable media is allowed by the Company.

### 9.3 REQUIREMENTS REGARDING EQUIPMENT

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

### 9.4 DISPOSITION OF EXCESS EQUIPMENT

Company laptops, that have been decommissioned from Company use, are reset to factory settings and sold to RightCapital employees as part of the “Used MacBook Pro BuyBack Program”. The purpose of this benefit was to allow active employees to purchase MacBook laptops at a significant discount.

Prior to being sold, all MacBooks undergo the following checks:

- The machines are decommissioned from Apple Managed Account.
- The machines are factory reset.
- All data is erased.
- Serial number is removed from company database and reassigned.



# 10 Change Management

---

## Statement of Policy

To ensure that Company is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems. Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

## Procedure

1. The IT staff or other designated Company employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
  - a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component or electronic health record (EHR) updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

# 11 Audit Controls

---

## **Statement of Policy**

To ensure that Company implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems. Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

The Company is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities. As such, the Company will continually assess potential risks and vulnerabilities to information in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

## **Procedure**

1. See policy entitled Information System Activity Review for the administrative safeguards for auditing system activities.
2. The Information Technology Services shall enable event auditing on all computers that process, transmit, and/or store information for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of patient data being accessed for each attempted access. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.
3. The Company shall utilize appropriate network-based and host-based intrusion detection systems. The Information Technology Services shall be responsible for installing, maintaining, and updating such systems.

# 12 Information System Activity Review

---

## Statement of Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Company shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

## Procedure

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Company's information systems.
2. The Security Officer will identify individual(s) independent of IT personnel to be responsible for conducting reviews of Company's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately. These person(s) may be internal to RightCapital or external consultants.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
4. Such reviews shall be conducted annually. Audits also shall be conducted if Company has reason to suspect wrongdoing. In conducting these reviews, reviewers shall examine audit logs for security-significant events including, but not limited to, the following:
  - a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
  - b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
  - c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
  - d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.
5. Reviewers shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to

Company's administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).

# 13 Business Continuation Plan

---

## Statement of Policy

RightCapital company policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all the firm's books and records, and allowing our customers to use our technology solution.

## Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our firm's ability to communicate and do business, such as a fire in our building. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption. Our response to an external SBD relies on other organizations and systems.

## Data Back-Up and Recovery

All your data is backed up daily. RightCapital maintains at least 30 days of backup data at any given time. In addition, we continuously take snapshots of the database. RightCapital can restore data to any point in time between the earliest backup and typically within 5 minutes of the current time.

RightCapital replicates customer data to at least two different locations at any given time to protect against failure or local disaster. The RightCapital platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. RightCapital reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

## Operational Risk Assessments

In the event of an SBD, we will immediately identify what means will permit us to communicate with our customers, employees, critical business constituents, critical banks, critical counterparties and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options we will employ will include *our website, telephone voice mail, secure email, etc.* In addition, we will retrieve our key data as described in the section above, Data Back-Up and Recovery.

## Disaster Recovery and Emergency Mode Operations Plan

- a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:
  - i. Restoring or recovering any loss of critical business data and/or systems necessary to make critical business data available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
  - ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an

emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.

- b. The disaster recovery and emergency mode operation plan shall include the following:
  - i. Current copies of the information systems inventory and network configuration developed and updated as part of Company's risk analysis.
  - ii. Current copy of the written backup procedures developed and updated pursuant to this policy.
  - iii. Identification of an emergency response team. Members of such team shall be responsible for the following:
    - 1. Determining the impact of a disaster and/or system unavailability on Company's operations.
    - 2. In the event of a disaster, securing the site and providing ongoing physical security.
    - 3. Retrieving lost data.
    - 4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.
    - 5. Taking such steps is necessary to restore operations.
  - iv. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of Company's risk analysis
  - v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:
    - 1. Members of the immediate response team,
    - 2. Facilities at which backup data is stored,
    - 3. Information systems vendors, and
    - 4. All current workforce members.
- c. The disaster recovery team shall meet on at least an annual basis to:
  - i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Company;
  - ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and

- iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

## 14 Security Awareness and Training

---

### Statement of Policy

To establish a security awareness and training program for all members of Company's workforce, including management.

All workforce members shall receive appropriate training concerning the Company's security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

### Procedure

- a. Security Training Program
  - i. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation for all training activities.
  - ii. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of addition of new hardware or software, and increased threats.
- b. Security Reminders
  - i. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.
  - ii. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.
- c. Protection from Malicious Software

- i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
  - a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
  - b) The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
  - c) Instructions to never download files from unknown or suspicious sources,
  - d) Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
  - e) The importance of backing up critical data on a regular basis and storing the data in a safe place,
  - f) Damage caused by viruses and worms, and
  - g) What to do if a virus or worm is detected.
- d. Password Management
  - i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:
    - a) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.
    - b) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
    - c) A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.
    - d) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency) or individuals, including family members.
    - e) Passwords must not be written down, posted, or exposed insecurely, such as on a notepad or on the workstation.
    - f) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
    - g) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.



# 15 Security Management Process

---

## Statement of Policy

To ensure the Company conducts an accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality and integrity.

Company shall conduct an accurate and thorough risk analysis to serve as the basis for Company's Security Rule efforts. The company shall reassess the security risks and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices and technological advancements.

## Procedure

- a. The Security Officer shall be responsible for coordinating the Company's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.
- b. The risk analysis shall proceed in the following manner:
  - i. Document Company's current information systems.
    - a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization's information system network is configured.
    - b) Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.
    - c) For each application identified, identify each licensee (i.e., authorized user) by job title and describe how authorization is granted.
    - d) For each application identified:
      - i) Describe the data associated with that application.
      - ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
      - iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
      - iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.
      - v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

- vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.
- e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") created, received, maintained, or transmitted by Company. Consider the following:
  - i) Natural threats, e.g., earthquakes, storm damage.
  - ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
  - iii) Human threats
    - a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls
    - b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment
    - c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail
    - d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction
  - iv) Identify and document vulnerabilities in Company's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to information, denial of service, or repudiation (*i.e.*, the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.
- f) Determine and document probability and criticality of identified risks.
  - i) Assign probability level, *i.e.*, likelihood of a security incident involving identified risk.
    - a. "Very Likely" (3) is defined as having a probable chance of occurrence.
    - b. "Likely" (2) is defined as having a significant chance of occurrence.
    - c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.
  - ii) Assign criticality level.
    - a. "High" (3) is defined as having a catastrophic impact on the medical Company including a significant number of medical records which may have been lost or compromised.

- b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the Company which may have been lost or compromised.
      - c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.
    - iii) Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.
  - g) Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high-risk scores, as well as specific security measures and safeguards required by the Security Rule.
  - h) Develop and document an implementation strategy for critical security measures and safeguards.
    - i) Determine timeline for implementation.
    - ii) Determine costs of such measures and safeguards and secure funding.
    - iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
    - iv) Make necessary adjustments based on implementation experiences.
    - v) Document actual completion dates.
  - i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.
- c. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Follow-up evaluations shall include the following:
- i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.
  - ii. Analysis to assess adequacy of controls within the network, operating systems, and applications. As appropriate, Company shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

# 16 Employee Background Checks

---

At RightCapital, reference checks are conducted on all job applicants using a third-party agency. The information collected as part of the reference check includes, but is not limited to, research of OFAC databases, the applicant's past employment (minimum prior 2 employers), full education record, residency and location for the past five years, any criminal record (minimum past seven years), and credit check, subject to provisions 2-4 below. The background check may also seek references to determine candidates' character, reputation, etc. This process is conducted to verify the accuracy of the information provided by the applicant.

RightCapital will ensure that all background checks are held in compliance with all federal and state statutes, such as the Fair Credit Reporting Act. For example, the Americans with Disabilities Act prohibits organizations from collecting non-job-related information from previous employers or other sources. Therefore, the only information that can be collected is that pertaining to the quality and quantity of work performed by the applicant, the applicant's attendance record, education, and other issues that can impact the workplace.

RightCapital or the third-party agency acting on behalf of RightCapital may make inquiries regarding criminal records during the pre-employment stage, however, as part of Title VII of the Civil Rights Act of 1964, this information cannot be used as a basis for denying employment, unless it is determined to be due to job-related issues or business necessity.

RightCapital or the third-party agency acting on behalf of RightCapital can collect credit information on applicants consistent with the guidelines set forth by the Fair Credit Reporting Act (FCRA). The Fair Credit Reporting Act requires organizations to obtain a candidate's written authorization before obtaining a credit report. When doing this RightCapital or the third-party agency acting on behalf of RightCapital will:

- Certify to the consumer-reporting agency that the employer is in compliance with the FCRA and will not misuse the information it receives.
- Disclose to the applicant or employee, on a separate form, its plans to obtain a consumer or investigative consumer report and that the information received will be used solely for employment purposes.
- Obtain written authorization from the applicant or employee.
- Inform the individual of his or her right to request additional information on the nature of the report and the means through which such information may be obtained.
- Inform the applicant that the report will include information about the individual's character, general reputation, personal characteristics, etc.
- Provide the individual with a summary of his or her rights under the FCRA.

If the results of the credit check are negative, RightCapital will inform the applicant that it plans on taking adverse action, provide the applicant with a Statement of Consumer Rights from the FTC before adverse action, provide the applicant the opportunity to review a copy of their credit report, and advise the applicant of their rights to dispute inaccurate information. Applicants will be granted reasonable time to contest the information (approximately 3-5 days).

The Company will conduct background checks in compliance with the federal Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), and all other applicable local, state, and federal laws and regulations. Applicants and employees may request and receive a copy of the requested

"investigative consumer reports."

A reported criminal offense conviction will not necessarily disqualify a candidate from employment. The nature and seriousness of the offense, the date of the offense, the surrounding circumstances, rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring, or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached. The Company will follow FCRA requirements, other applicable statutes, and Company procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

The Company reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.

Background check reports shall be maintained in separate, confidential files and retained in accordance with the Company's document retention procedures.

## **Record Keeping**

RightCapital guarantees that all information obtained from the reference and background check process will only be used as part of the employment process and kept strictly confidential. RightCapital will maintain a log that includes name, position, and the date of the background check for all applicants. Only appropriate personnel at RightCapital will have access to this information.

# 17 Breach Notification Procedures

---

## Reporting of the breach

All Information security incidents should be reported immediately to manager of information technology, as the primary point of contact.

The report should include full and accurate details of the incident, including who is reporting the incident; what type of data is involved (not the data itself unless specifically requested); if the data relates to people and if so, how many people are involved.

The Information technology team is responsible for maintaining a confidential log of all information security events.

## Investigation and Response

The Information technology team will review the report, and where appropriate, create a Response Team. Information technology will lead the Response team and membership will depend on the type and severity of the incident. The response team will be responsible for investigating the circumstances and effect of the information security incident. An investigation will be started into material breaches within 24 hours of the breach being discovered, where practicable.

The investigation will establish the nature of the incident, the type of data involved, whether the data is personal data relating to individuals or otherwise confidential or valuable. If personal data is involved, associated individuals must be identified and, if confidential / valuable data is concerned, what the legal and commercial consequences of the breach may be.

The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss. This will include risk of damage and/or distress to individuals and the institution.

The response team is responsible to assign incident category using the guidance below.

The response team is responsible for formally documenting the incident and associated response. This information will (as a minimum) be subject to review by the CTO with serious incidents reviewed by Senior Management Team.

## Containment and Recovery

The Response team will determine the appropriate course of action and the required resources needed to limit the impact of the breach. For instance, this may require isolating a compromised section of the network; alerting relevant staff or contractors; changing access codes/locks or shutting down critical equipment.

Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

For incidents that involve a suspected or actual criminal offence, all efforts will be made to preserve evidence integrity.

## Escalation & Notification

The details of the escalation and notification process are summarized below.

The response team is responsible for initial assessment of an incident's severity based on the scope, scale and risk of the incident.

This preliminary decision is then reviewed by the director of Information Technology team and business partners. Review includes scope of incident, impact on partners, and reputational risk.

If at this stage the incident is assigned as category 1 or 2, then the Company Senior Management Team will be notified.

If a personal data breach has occurred of sufficient scale, the response team will notify CTO and CEO.

If the breach is deemed of sufficient seriousness, and concerns financial data, notice of the breach will be made to affected customers to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks, and will be undertaken by the Information Technology Team. Collaboration with the Police or other authorities may be required for serious events.

If the incident is assigned as category 1 or 2, a reputational risk evaluation will be done and reviewed with Senior Management. This will be done in conjunction with business partners where appropriate.

## **Review**

Once the incident is contained a thorough review of the event will be undertaken by the Information technology Team, to establish the cause of the incident, the effectiveness of the response and to identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter. Targeted training may be offered to the department affected. Review may include technical changes, process changes, and/or evaluation of reputational impact.

All information security incidents will be subject to summary review by the Company's Senior Management Team so that any weaknesses or vulnerabilities that may have contributed to the incident can be identified, documented and resolved.

## 18 Policy Governance

---

The following table identifies who within the Company is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Responsible</b>	Song Chen, CTO
<b>Accountable</b>	Shuang Chen, CEO
<b>Consulted</b>	Carly Lavin, Head of Operations
<b>Informed</b>	Dain Runestad, VP of Product