revenue analytics

Data Security and Privacy

Revenue Analytics manages the security and privacy of information stored or transmitted electronically by its information systems. Our policies are designed to prevent, detect, contain and correct security violations by establishing procedures that assist in (i) identifying and evaluating risks and vulnerabilities present in Revenue Analytics' operations-related information systems and operations ("Risk Analysis"); and (ii) monitoring and managing these risks ("Risk Management").

These policies apply to Revenue Analytics' computer systems that contain or access electronic data, including, but not limited to, local on premise network servers, cloud network servers, desktop computer systems, laptops, handheld devices, backup management systems, and infrastructure devices.

Risk Analysis

In order to identify and evaluate risks inherent in Revenue Analytics' information security system, risk assessments are performed on an annual basis. The result of the risk assessment is a plan that documents changes necessary to implement control procedures.

Risk Management

Risk Management is an ongoing activity that involves monitoring and managing the risks identified and evaluated during the Risk Analysis process to ensure that such risks are minimized to a level deemed acceptable by our Management and our Clients.

As part of the Risk Management process, Revenue Analytics undertakes the following tasks:

a. Monitoring Safeguards. Revenue Analytics has established administrative, physical, and technical safeguards to reduce the risk of security breaches caused by untrained personnel, unauthorized access, improper handling of machines, and failure to be prepared for contingency or emergency situations. Revenue Analytics monitors the effectiveness of these safeguards by providing appropriate training, controlling access to information technology systems, maintaining systems and planning for emergencies.

b. Yearly Review. An Internal Audit Team performs annually more comprehensive reviews of Revenue Analytics' information technology security system including controls testing with a review of findings with Management. All results as well as necessary changes to current policies and procedures will be documented and included in annual training meetings.

Workforce Security

Revenue Analytics protects the confidentiality and integrity of electronic information and permit only authorized individuals access to such information. This policy applies to all members of Revenue Analytics' workforce regardless of where they are conducting business.

Authorization and Supervision.

Revenue Analytics has implemented the following procedures to ensure appropriate authorization and supervision over its employees:

a. Authorization. The IT Department assigns unique user IDs to all personnel. Access rights shall be granted in accordance with the Access Control Policy. Also they shall modify or terminate access rights as required by a change in the personnel's job position or as required by an emergency or temporary circumstance.

b. Supervision. Management may authorize maintenance personnel and other employees access to areas where protected information may be stored only under certain conditions and with adequate supervision. Management restricts access to its facilities by contractors and visitors in accordance with the Facility Access Controls Policy. Human Resources provides training to promote effective supervision of employees who work with and/or in proximity to protected information.

Termination Procedures.

Human Resources and/or the appropriate member of Management performs the following procedures for terminating access to electronic information when the employment of a workforce member ends:

1. Recover all keys, identification cards, physical tokens, and any other objects that facilitate physical access to office, building, and equipment.
2. Recover any information regarding Revenue Analytics and any property of Revenue Analytics that may be in the terminated workforce member's possession. Human Resources and/or the appropriate member of Management may require that terminated workforce members are escorted while they pack their belongings and as they leave the premises.
3. Notify the IT Department to deactivate user identification numbers, passwords, tokens, and other electronic access codes.

Security Awareness and Training

All Revenue Analytics employees receive training on security policies and procedures with respect to safeguarding electronic information as reasonable and appropriate to carry out their functions within or on behalf of Revenue Analytics.

Responsibility for Training.

Human Resources in conjunction with Management oversee the training of employees regarding security policies and procedures.

Training.
Each newly hired employee is trained on the policies and procedures during their first week of employment. After initial training, employees will complete additional training periodically in response to environmental and operational changes affecting the security of electronic information and, at a minimum, on an annual basis. In addition, in the event of a material change in security policies and procedures, workforce members whose functions are affected by the material change shall complete additional training within a reasonable period of time, generally 30 days after the material change becomes effective.

Security Incident Procedures
Revenue Analytics responds to security incidents and modifies its security program to reduce the likelihood of future incidents and as part of our efforts to identify and respond to suspected or known security incidents; to mitigate, to the extent practicable, harmful effects of security incidents that are known to Revenue Analytics; and to document security incidents and their outcomes.

This policy shall apply to all computer systems that contain or access electronic PHI, including, but not limited to, local and cloud servers, desktop computer systems, laptops, handheld devices, data management systems and infrastructure devices.

Revenue Analytics' computer incident response team ("CIRT") is comprised of the Senior Manager of IT, the Partner of HR and Administration, the Vice President of Data Engineering and the Vice President of Managed Analytics. The CIRT is charged with the responsibility of identifying, evaluating and responding to security incidents.

Response Plan.
The response plan sets guidelines for: (a) reporting, (b) documenting, (c) notifying others of, and (d) evaluating and responding to, security incidents.

a. Reporting Security Incidents. As part of new hire training classes, workforce members shall learn how to determine what constitutes suspicious activity and how to report such activity.
b. Documenting Security Incidents. The IT Department documents security incidents reported by employees or Management in an activity log. Each activity log shall set forth a summary of the incident, actions taken, contact information for involved parties, a list of evidence gathered, comments from incident handlers, and subsequent steps to be taken. The activity logs shall be updated on a continuous basis by IT or a member of CIRT. The IT Department shall ensure that the activity logs are kept in a secure location and shall prohibit access by anyone other than the IT Department, the members of CIRT, or Management.

c. Notifying Others of Security Incidents. The IT Department shall contact the members of CIRT when a security incident occurs. The CIRT shall contact Management and the legal and public relations departments if deemed necessary by Management.

d. Evaluating and Responding to Security Incidents. The IT Department and CIRT shall have criteria for classifying the severity of a reported security incident (critical, high, medium, low, or no threat) and the procedures to be followed for each level of security incident. The IT Department shall classify each incident reported and shall review the classification with Management, who shall provide additional instruction as necessary. A list of general procedures to follow are outlined below. These general procedures shall be supplemented, amended, or replaced at any time as agreed by the IT Department, CIRT and Management.

Response Team.

The responsibilities of CIRT shall include:

1. identifying and escalating incidents within the organization;
2. communicating with entities that can assist in diagnosis or in contacting other affected websites;
3. evaluating the extent of exposure;
4. providing security announcements, if deemed necessary;
5. assisting in the containment of damage;
6. preserving evidence;
7. restoring the information system;
8. documenting the incident; and
9. performing a final review.

In addition, CIRT shall perform on a regular basis activity such as:

1. training other workforce members to recognize and report security incidents;
2. conducting systems vulnerability assessments;
3. monitoring current technology reports and sending out advisories;
4. implementing intrusion detection devices and monitoring the resulting reports and activity logs; and
5. distributing and managing the installation of patches and updated virus software.

Protective Measures.

CIRT ensure that the following protective measures are implemented:

a. Back-ups. CIRT shall ensure that Revenue Analytics maintains adequate back-ups of its data and customized systems and software configurations. CIRT ensures that the back-up tapes are sufficient to restore Revenue Analytics' computer information system and to capture all important data. In addition, CIRT shall ensure that copies of back-up tapes are stored offsite in a secure location.

b. Systems Diagrams. CIRT shall ensure that updated systems diagram are maintained to reflect current system architecture, including: a list of hardware currently in place, a list of software installed on each machine, vendor manuals/user documentation, and a diagram of all the various connections and interconnections between hardware and equipment and between hardware and software. CIRT shall ensure that all labels are clearly marked, signed, and dated. CIRT shall ensure that enough information is readily available and safely secured so that Revenue Analytics' computer systems can be rebuilt or restored as soon as practicable.
c. Preventive Software. The IT Department shall run virus detection software on a weekly basis to ensure that no viruses have been introduced into the computer information system and to ensure that no unauthorized modifications have been made to any application source code. Information Resources shall update the virus checking software as updates become available.
d. Original Applications. The IT Department shall ensure that all vendor original software applications are stored offsite in a secure location, along with copies of customized configurations. The IT Department shall ensure that the uncontaminated copies are installed in the event the CIRT or Management shall deem a rebuild is warranted.
e. Activity Logs. The IT Department shall maintain activity logs that record when programs are installed, when configurations are added, and when security incidents occur. CIRT shall review these detailed records on a monthly basis and shall immediately act on any unusual activity.

Response Procedures.
In the event of a security incident, the members of CIRT shall follow the general procedures listed below:

a. Identify and Document Incident. The IT Department shall review reported security incidents, classify each incident and document each incident in the activity log. The CIRT shall assist as needed.
b. Notify Team Members. The IT Department shall maintain a list of e-mail addresses and telephone numbers (including office, home, and cell numbers) for members of CIRT and Management. The IT Department shall contact everyone on this list after performing an initial review of the security incident report.
c. Evaluate/Determine the Extent of Exposure. The IT Department and CIRT shall work together to identify, to the extent possible, the specific nature of the problem and the potential threat of exposure to damages or loss of information by Revenue Analytics.
d. Coordinate a Response. After consultation with CIRT, the IT Department shall take the steps necessary to contain the threat and to restore Revenue Analytics' system to normal operations. CIRT shall notify other members of the organization who need to know of the security incident, such as end users who cannot

perform their daily tasks. Any notification to end users shall contain the following information:

i. what is happening to the network and computer system;
ii. why the system or certain applications are being shut down;
iii. what users can and cannot do;
iv. when service will be restored; and
v. a promise to provide ongoing updated information.
vi. CIRT shall ensure that updated notices are disseminated on a frequent basis until the problem has been resolved.

Restore and Recover.
The IT Department shall make adjustments to or re-build the system as directed CIRT and Management. If a rebuild is required, the IT Department shall first re-install an original version of the operating system, then original copies of the vendor software, then any customized modifications, followed by data loaded from back-up tapes created prior to the security incident.

Document All Responsive Measures Taken.
Each member of the IT Department as well as CIRT shall document his or her actions and observations in the activity logs so that the other members of CIRT or Management can see the current status of the security incident, which measures have been taken, and which measures remain pending. The IT Department shall ensure that the activity logs are maintained electronically as well as in hard-bound notebooks with preprinted page numbers. The hard-bound notebooks may include hard copies of the electronic version, provided that such hard copies are printed on a routine basis and tightly affixed in the hard-bound notebooks. The IT Department shall also ensure that phone calls and discussions regarding a security incident are recorded in the activity logs, including information regarding who was present, what was discussed, and the outcome of the conversation.

Disseminate Follow-up Information.
CIRT shall ensure that individuals within Revenue Analytics who need to know the status of the security incident and measures taken remain informed during the security incident. Upon resolution, CIRT shall distribute a final notice to that effect.

Conduct Final Review.
After the problem has been contained and systems have returned to normal operations, CIRT shall conduct a final review of the activity logs and analyze whether the measures taken were appropriate for the particular security incident or whether other measures should have been taken. CIRT shall analyze the effectiveness of the efforts by:

1. reviewing activity logs for adherence to established procedures;
2. determining if any warning signs were evident and recorded in the activity logs;

3. determining if the incident had caused damage before it was detected;
4. determining if the actual cause of the incident was accurately identified and corrected; and
5. identifying which measures, if any, could have prevented the incident.

CIRT shall prepare a report documenting it conclusions and proposed changes, and submit the report to Management. Based on this report, Management may request changes to the Response Plan or Response Procedures, which CIRT and the IT Department review and implement as deemed advisable and as soon as practicable. The IT Department and CIRT shall cooperate with additional instructions from law enforcement or federal agencies to the extent authorized by Management and the legal department.

Contingency Operations Plan.
Revenue Analytics has established procedures for responding to an emergency or other occurrence that damages Revenue Analytics' information systems that contain electronic protected information, including implementation of a Data Backup Plan, a Disaster Recovery Plan and an Emergency Mode Operation Plan.

Data Backup Plan.
The CIRT shall oversee the implementation of the following procedures that provide for the creation and maintenance of retrievable exact copies of electronic information.

a. Personnel Responsibility. The IT Department shall establish specific backup schedules and procedures for Revenue Analytics' networks and computer systems.
b. Daily Backups. The IT Department shall back up all software, applications, files, data, and messages related to its operations stored on premise servers and cloud servers.
c. Backup Validation. The IT Department shall validate the accuracy, completeness and integrity of the backup performed each night. The IT Department shall act to promptly resolve errors shown by the validation process and shall either resolve the errors or seek outside technical support to assist in the resolution of errors in the backup process.
d. Onsite Storage. The storage media from the previous day or current week shall be stored onsite in an area secured in a safe. The IT Department as well as CIRT shall have the combination to this safe.
e. Offsite Storage. The IT Department shall approve an environmentally secure offsite location that provides adequate security and protection from fire and other disasters for storage of a copy of Revenue Analytics' backup media.
f. Restoration of Lost Data. For backup data stored offsite, the IT Department shall develop a plan for the retrieval of such backup data. The IT Department shall ensure that any necessary backup data is retrieved from the offsite location

using the most expedient means practical in case of a partial or complete system failure.

Disaster Recovery Plan.

CIRT in conjunction with the IT Department shall oversee the implementation of the following procedures to restore any loss of data in the case of a catastrophic event such as an emergency, fire, vandalism, system failure, or natural disaster.

a. Disaster Assessment. Once a disaster has occurred, the IT Department shall assess the effect of the disaster on Revenue Analytics' information system to determine any lost functionality and loss of data. If it is determined that data has been lost, the IT Department should consult with CIRT on whether to implement this Disaster Recovery Plan.
b. Personnel Responsibility. The IT Department is responsible for implementation of this Disaster Recovery Plan and the restoration of any lost data.
c. Secure Facilities. In the event of a catastrophic event, Revenue Analytics security personnel shall immediately ensure that all facilities housing Revenue Analytics' information systems remain secure under the circumstances. Revenue Analytics security personnel shall limit access to facilities to only authorized personnel meant to assist in disaster recovery.
g. Password Access. Director-on-call and other administrators for backup and restoration shall have access to system passwords to perform restores of necessary systems and data.
h. Onsite Backup Data. The Director-on-call shall ensure that the administrators for backup and restoration have access to any backup media stored onsite if necessary to restore software, applications, information and data to UTD information systems.
i. Systems Architecture and Diagrams. The IT Department shall develop and maintain detailed descriptions of Revenue Analytics' main system hardware components to help rebuild the system in the event of disaster, maintain updated profiles for each system configuration and maintain lists of installed software, including current installed patches, drivers, and O/S distribution media.
j. Offsite Storage. The IT Department shall retrieve all necessary backup files stored offsite.
k. The IT Department shall oversee the loading and testing of backup files and getting the network and computer systems operational and back online.

Emergency Mode Operation Plan.

CIRT shall oversee the implementation of the following procedures to enable continuation of critical business processes for protection of the security of electronic information while operating in emergency mode.

a. Emergency. For the purposes of this Emergency Mode Operation Plan, an "Emergency" shall be defined as an incident that either disables, wholly or partially, or substantially impairs Revenue Analytics' central computing system or any computer system or network that contains or allows access to electronic information for a period of 48 hours.

b. Determination of Emergency. When an incident occurs, the IT Department shall assess the situation and determine whether to declare an Emergency and institute this Emergency Mode Operation Plan. Revenue Analytics employees shall report any incident that results in or may result in an Emergency to the IT Department and/or CIRT.
c. Personnel. CIRT shall designate the workforce members who will serve as administrators for backup and restoration.
d. System Changeover. If the security of any network or computer system has been compromised as a result of the Emergency, the IT Department shall disable such network or computer system and operate only on secured systems.
e. Backup Servers. If necessary, the IT Department shall ensure that Revenue Analytics' backup servers containing critical security applications are brought online to safeguard and continue critical business processes, applications (such as firewalls), and virus protection software, that protect computer systems and networks that contain electronic information.
f. Assess the Damage to Computer Systems. The IT Department shall assess the extent of damages to Revenue Analytics' computer systems that enable continuation of critical business processes for the protection of electronic information and begin procedures to repair and bring the computer systems back online as soon as practical.
g. Notify Service Providers. The IT Department shall contact vendors for servicing any damaged computer systems to restore as soon as practical any damaged systems.
h. Operations. Revenue Analytics shall operate in emergency mode until the Emergency has ended and all computer systems that affect the protection of electronic information have either been restored to full capacity or replaced.

Testing and Revision Procedures.

a. Personnel Responsibility. The IT Department shall develop and implement testing procedures for any contingency operations plans.
b. Testing of Data Backup. The IT Department shall periodically test (no less than once every year) whether authorized persons can effectively access backup data stored onsite and offsite in a timely manner in order to restore any lost data.
c. Testing of Disaster Recovery Emergency Operations Procedures. The IT Department shall oversee the testing of procedures and components of the Disaster Recovery Plan and Emergency Mode Operation Plan. Any vulnerabilities identified in the Disaster Recovery Plan and Emergency Mode Operation Plan shall be addressed immediately.

Facility Access Controls

Revenue Analytics shall limit physical access to its electronic information systems and the rooms/closets in which they are housed.

Location of Servers and Databases.

a. The IT Department shall ensure that all on premise servers, routers, database systems, device management system hardware, and other servers used by Revenue Analytics are located in a room or an area within Revenue Analytics that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.
b. The IT Department shall ensure that all facilities housing Revenue Analytics' electronic information systems shall be secured by lock at all times. The following authorized personnel shall have access to these facilities: IT Department personnel, CIRT and Management.
c. Any other workforce members requiring access to facilities housing Revenue Analytics' electronic information systems shall request and receive permission from the IT Department.

Contingency Operations.

The IT Department shall implement the following procedures to allow facility access in the event of an emergency, disaster, or other occurrence resulting in lost data:

a. Secure Facilities. In the event of a disaster, Revenue Analytics security personnel shall lock down all facilities containing Revenue Analytics' electronic information systems and protected information in non-electronic form. Revenue Analytics security shall limit access to facilities to authorized personnel.
b. Access for Restoration Purposes. Revenue Analytics security shall permit access to all workforce members involved in the repair of electronic information systems and in the restoration of lost data in accordance with the Emergency Mode Operation Procedures and Disaster Recovery Procedures.
c. Back-up Data On-Site and Off-Site. Revenue Analytics security shall see that Revenue Analytics workforce members involved in Emergency Mode Operation Procedures and Disaster Recovery Procedures have access to rooms and areas containing any back-up data stored on- site or off-site.

Facility Security Plan.

Revenue Analytics shall implement the following procedures to safeguard facilities and equipment from unauthorized physical access, tampering, and theft.

a. Revenue Analytics shall maintain offices in buildings equipped with security personnel and video monitoring.
b. Revenue Analytics security shall routinely check to ensure that locked doors remain locked and that facilities remain secure.
c. Visitors shall be escorted by the person being visited while in the facilities if reasonable and practical.

Access Control and Validation Procedures.

Revenue Analytics shall implement the following procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision:

a. Unattended exterior doors shall be protected by locks, electronic locks, and/or badge readers.
b. Visitors to the facility who are business invitees shall present, upon request, positive identification.
c. If reasonable and practical, the person being visited shall accompany such visitors while in the facility.
d. Such visitors shall only be allowed access to common areas or areas necessary to perform the function for which the visitor is in the facility.
e. Unless maintenance and service personnel, such visitors shall not be allowed physical access to information systems, media containing electronic information, or records containing protected information. Management shall approve any exceptions to this procedure.
f. Electronic information systems or media containing electronic information shall be shielded from viewing by patients' visitors.
g. Management shall require that contractors performing work for Revenue Analytics wear badges issued by their employer. Access by contractors shall be limited to normal business hours. If a contractor's job requires access after normal business hours, a member of Revenue Analytics' workforce or security personnel shall be present.
h. Management shall provide contractors needing access to facilities containing protected information with any Security Policies and Procedures applicable to the area or the information being accessed. If a contractor violates Revenue Analytics' Security Policies and Procedures or exceeds or attempts to exceed the rights of temporary access granted pursuant to the procedures set out in this subsection, the violation should be reported immediately to Management.
i. Revenue Analytics team members who observe a person attempting to enter Revenue Analytics facilities by bypassing any security measure shall report that person to Revenue Analytics security personnel, CIRT, or Management.

Workstation Use

Revenue Analytics shall implement procedures that specify the proper functions to be performed on workstations and the manner in which those functions shall be performed.

This Workstation Use policy shall apply to all workstations that contain or have access to protected information, which include electronic computing devices, such as personal computers, laptop computers, personal digital assistants ("PDAs"), tablet computers, or devices that perform similar functions, and electronic media stored on electronic computing devices.

Proper Functions to Be Performed.

a. Revenue Analytics shall provide workstations to employees for the purpose of performing their job functions. Users of Revenue Analytics workstations shall be responsible for using workstations appropriately in conformance with this policy.
b. Users shall use workstations to perform the duties that are a necessary part of a workforce member's job function. Such functions include but are not limited to those functions as set out in the workforce member's job description.

Functions That May Not Be Performed.

a. Users shall not use workstations to access any confidential or proprietary information of Revenue Analytics that they do not have a need to know to perform a job-related function.
b. Users shall not use workstations to transmit any confidential or proprietary information of Revenue Analytics to any third party unless authorized by Management.
c. Users shall not download protected information from Revenue Analytics' information systems and store it on a workstation, except as necessary to perform job functions.
d. Users shall not attempt to evade the access rights granted to the User and shall not attempt to access any network, system, application, or data to which the User has not been granted access.
e. To protect against computer viruses from being transmitted onto workstations and into Revenue Analytics' electronic information systems, Users shall not download from the Internet any unauthorized programs or applications and shall not upload any unauthorized external software or data. Before a workforce member downloads programs or applications from the Internet or uploads any external software to a workstation, the User shall receive the approval of the IT Department.
f. Users of workstations shall not open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source and shall delete these attachments immediately because they may contain viruses, e-mail bombs, or Trojan Horse code.
g. Users shall not install non-Revenue Analytics hardware on any workstations unless approved by the IT Department or install unauthorized modems or other communications devices to the network.
h. Users shall not use a Revenue Analytics-owned workstation to engage in an activity prohibited by Revenue Analytics' employee handbook or Human Resources policies and procedures.
i. Users shall not engage in any activity that is illegal under local, state, federal, or international law while using Revenue Analytics-owned workstations.
j. Users shall not use Revenue Analytics-owned workstations for personal gain or for business-related purposes or functions unrelated to the User's job function.

k. Users shall not remove from Revenue Analytics' facilities electronic media that contains protected, confidential or proprietary Revenue Analytics information unless such removal is authorized by a User's supervisor and the User signs out the media.

Manner in Which Functions Are to Be Performed.

a. Users shall log onto the workstation using the User ID assigned to that User. Users shall not log onto a workstation using another person's User ID or password nor shall the User permit another person to log on with his or her User ID or password. Users shall not enter data under another User's unique User ID or password. Users shall not attempt to mask their identity while logged onto a workstation or Revenue Analytics' network. Furthermore, Users shall keep their User IDs and passwords confidential and shall change passwords as required by the system.
b. Users shall attempt to keep their computer monitors away from public viewing during use.
c. It is recommended that Users shall log off workstations or establish a password-protected screen saver before leaving the workstation unattended for more than 10 (ten) minutes.
d. Users shall not leave printers unattended when they are printing protected information or other confidential information. This procedure is especially important when two or more computers share a common printer or when the printer is located in an area where unauthorized personnel have access to the printer.
e. Hard-copy printouts of protected information shall only be made if needed for reasonable business purpose. Only the minimum necessary information shall be printed. The printouts shall be shredded and disposed of after use.
f. Users shall erase protected information from electronic media once no longer in use. A shredder is available to destroy any out of use disks.

Physical Attributes of Workstations.

a. The IT Department shall install on workstations a password-protected screensaver that requires Users to enter a User ID and password to access. The workstations shall have a time-out feature after a certain period of inactivity.
b. Revenue Analytics shall employ currently acceptable means by which to detect and prevent the spread of computer viruses, worms, Trojan Horses, or any other agents designed to alter or destroy data.
c. Workstations shall have anti-virus protection software that detects computer viruses, worms, Trojan Horses, and any other disabling agents. Users shall not disable the anti-virus software.
d. The anti-virus protection software shall be installed so that all attachments are scanned before downloading to a workstation and prevent the download of attachments containing viruses, worms, Trojan Horses or other disabling agents.

e. Users shall scan for viruses or other disabling agents whenever external files are placed on any workstation that accesses Revenue Analytics' internal network and computer system.
f. The IT Department shall configure servers to perform a single function, if possible.

Workstation Security
Revenue Analytics shall implement safeguards to restrict access to workstations that access electronic protected information only to authorized users.

This workstation use policy shall apply to electronic computing devices that have access to PHI, including personal computers, laptop computers, personal digital assistants ("PDAs"), tablet computers, or other devices that perform similar functions, and electronic media stored on electronic computing devices.

Portable Devices.

a. Portable computing devices, including laptop computers, personal digital assistants (PDAs), portable storage devices, etc., while at Revenue Analytics' facilities, shall be locked up at the end of each workday.
b. Users shall secure portable computing devices when such devices are used outside of Revenue Analytics' facilities.
c. If a User accesses protected information from a portable computer device, the device shall be password-protected so that Users must enter a password before access is granted. The protected data on the portable computer device must be encrypted using Revenue Analytics-approved digital encryption methodology.
d. If accessing protected information from portable computing devices, Users shall prevent the information from being viewed by others.

Desktop Devices.

a. Users shall logout of and shut down all desktop devices at the end of the day.
b. If a User accesses protected information from a desktop computer device, the device shall be password-protected so that Users must enter a password before access is granted. The protected data on the portable computer device must be encrypted using Revenue Analytics-approved digital encryption methodology.
c. If accessing protected information from portable computing devices, Users shall prevent the information from being viewed by others.

Device and Media Controls
Revenue Analytics shall implement reasonable and appropriate controls to govern the receipt and removal of hardware, to govern electronic media that contain electronic protected information into and out of Revenue Analytics' facilities and within Revenue Analytics' facilities, and to implement methods to dispose of electronic information.

This policy shall apply to Revenue Analytics-owned or leased hardware containing electronic protected information, including on premise and cloud servers, PCs, laptops, personal digital assistants (PDAs), etc. and electronic media containing protected information, including hard disk drives, DVDs, CDs, flash drives, pen drives, USB drives, diskette tapes, floppy disks and other portable storage devices.

Receipt of Hardware or Electronic Media Containing Protected Information.
The following procedures shall govern the receipt of hardware or electronic media containing protected information from outside entities or persons:

a. The Project Manager or a member of the Data Engineering team shall receive any hardware or electronic media containing protected information on Revenue Analytics' behalf. If any Revenue Analytics workforce member receives hardware or electronic media containing protected information, the workforce member shall notify the project manager.
b. Upon receipt of hardware or electronic media containing protected information, the Project Manager shall log who received the hardware or electronic media, a description of the hardware (including the serial number) or type of media, from whom received, the client to whom the protected information pertains, the reason for receiving, and the date of receipt.
c. If the hardware or electronic media containing protected information is subsequently returned to the person or entity who initially gave it to Revenue Analytics, the date of return, to whom returned and the person returning it shall be recorded in the log described in the paragraph above.

Movement of Hardware and Electronic Media from Revenue Analytics' Facilities.

a. Revenue Analytics workforce members shall not remove from Revenue Analytics' facilities any hardware or electronic media containing electronic protected information nor download protected information to any computer, device, or network that is not located in Revenue Analytics' facilities without the approval of the Project Manager. Such approval shall only be granted if the hardware, electronic media or downloaded protected information is necessary for the performance of a job-related function on Revenue Analytics' behalf.
b. The Project Manager shall not grant any request to remove hardware or electronic media containing protected information or download protected information unless it is necessary to perform a job function for Revenue Analytics and the request has the approval of the client.
d. Revenue Analytics workforce members shall return the hardware or electronic media or erase the downloaded protected information when the job function is completed. If not erased, the workforce member shall safeguard the information accordingly.
e. Revenue Analytics workforce members may remove from Revenue Analytics' facilities personal portable computing devices (notebook or laptop computers,

pocket computers, personal digital assistant devices (PDAs) or other similar computing devices) that contain or are capable of accessing protected information provided that the provisions of this Policy are adhered to. The following additional requirements shall be in force:

i. The portable computing device shall be password-protected, requiring that the workforce member enter a password before accessing any protected information.
ii. The protected information on portable computing devices shall be encrypted.
iii. The workforce member shall be responsible for the security of the device and protecting the confidentiality of any protected information in accordance with this Policy.
iv. Revenue Analytics workforce members shall promptly report the loss or theft of any hardware, electronic media, or any protected information data stored on the hardware or electronic media to Project Manager and the appropriate members of Management.

Final Disposal of Electronic Protected Information.

Removal Standard.
The IT Department shall ensure that protected information subject to final disposition by Revenue Analytics is disposed of by using a method that ensures the protected information cannot be recovered or reconstructed.

Retrievable Copy.
The IT Department shall ensure that a retrievable back-up copy is made before submitting hardware or electronic media for disposal of electronic protected information if it contains the only copy of the electronic protected information that is required or needed by Revenue Analytics.

Hardware.
The IT Department shall be responsible for the final disposal of hardware that contains protected information or the final disposal of electronic protected information on hardware using the following methods:

a. If Revenue Analytics is deleting protected information but not the hardware, the IT Department shall remove protected information from hardware using initialization utilities installed on such hardware that are designed to permanently remove data from memory locations.
b. If all data is being removed from the hardware, the IT Department shall reformat and overwrite memory locations using an appropriate overwriting program or degauss the hardware if practical and appropriate.
c. The IT Department shall maintain a log of such data destruction that lists the device, the date of destruction, the workforce personnel authorizing the

destruction, general description of the protected information (if available), and the identity of the workforce personnel performing the destruction.

d. The IT Department shall remove all protected information from hardware being sold, donated, replaced, or destroyed so that it cannot be recovered or reconstructed using appropriate disposal techniques.

Electronic Media.
The IT Department shall be responsible for the final disposal of protected information on electronic media and/or the final disposal of the electronic media on which it is stored. Although Users may erase any protected information contained on electronic media, any media containing protected information to be disposed of on a final basis by Revenue Analytics shall be submitted to the IT Department for deletion.

a. The IT Department shall delete protected information stored on electronic media using utilities that are designed to permanently remove data from memory locations.
b. The IT Department shall destroy all data on electronic media intended to be re-used, sold, donated, replaced or destroyed using appropriate disposal techniques.

Media Re-use.
Media shall not be re-used for any purpose other than storing other protected information unless all protected information has been removed from the media before such re-use. However, if the media is re-used as part of Revenue Analytics' data back-up procedures or disaster recovery, such media shall not be subjected to these procedures before each re-use.

Users shall not re-use CDs, diskettes or other electronic media on which protected information has been stored for any purpose other than storing other protected information before the protected information is removed by the IT Department using one of the approved methods.

Revenue Analytics shall implement the following procedures to maintain a record of the movements of hardware and electronic media and any person responsible for such movement:

a. UTD shall employ inventory controls and take inventory on an annual basis throughout the enterprise to track hardware and its location within the facility.
b. The IT Department shall maintain a log of any media containing electronic protected information that has been removed from Revenue Analytics' facilities showing the type of media, workforce member removing the media, the date of removal, the person approving the removal, and the date the media was returned.

Audit Controls

Revenue Analytics shall record and examine activity in information systems that contain or use electronic protected information for the purposes of identifying suspect activity, identifying high-risk activity, identifying security breaches, responding to potential security weaknesses, and assessing Revenue Analytics' security program.

This policy shall apply to all computer systems that contain or access electronic PHI, including, but not limited to, local and cloud servers, desktop computer systems, laptops, data management systems, and network and storage devices.

Implementation of Audit Control Mechanisms.

a. The IT Department shall ensure that all computer systems that contain or access electronic protected information have in place audit controls for recording and examining activity.
b. The IT Department shall configure any new computer system received by Revenue Analytics to record or examine activity on the system, if not already contained on the new system. The IT Department shall not bring this new system online until audit controls have been established.

Activity to Be Logged.
The IT Department shall implement software on Revenue Analytics information systems (including applications or processes) containing or accessing electronic protected information that records system activity such as logon, logoff, file access, file activity, attempted logons, and failed logons concurrent with the system activity.

Information Logged.
The implemented audit control mechanism shall identify:

a. Who or what is accessing data;
b. When the data is accessed;
c. What data was accessed;
d. The activity that occurred (read only, add, delete, modify data);
e. Whether data is accessed by anyone outside of Revenue Analytics; and
f. Successful and unsuccessful login attempts.

Respond to System Activity.
The IT Department shall promptly respond to any observed or reported suspect activity. The IT Department should follow previously described security procedures with respect to any suspect activity.

Audit Trails.
The IT Department shall maintain audit trails showing system activity for a minimum of 2 years. Audit trail information and reports containing audit trails shall remain confidential. The audit trail shall contain:

a. The type of event;

b. The User associated with the event;
c. The date the event occurred;
d. The method or program used to access the information system; and
e. The activities undertaken with respect to the data accessed.

Review System Activity.
CIRT shall oversee the review of audit trails at least monthly. The IT Department shall work with the CIRT in reviewing the audit logs. Specifically, the IT Department shall identify for CIRT any suspect activity and any potential security weaknesses. CIRT shall be responsible for determining whether an external review is necessary for Revenue Analytics' audit control system.

Transmission Security
Revenue Analytics shall safeguard electronic protected information transmitted over an electronic communications network from unauthorized access.

This policy shall apply to Revenue Analytics' network and all computer systems from which or to which electronic information is transmitted.

Implementation of Procedures.
The IT Department shall oversee the implementation of technical solutions that safeguard electronic information when transmitted over electronic communications networks.

Internet Communications.
The IT Department shall use secure socket layer (SSL) technology on any web page in which electronic information may be entered or received. For all exchange of data over the internet between computer devices on Revenue Analytics internal networks and cloud servers, the IT Department will maintain firewalls at both ends and utilize AES-128 or higher encryption and SHA1 authentication.

Sending Electronic Information via Email.
Any electronic information sent via emails must be in accordance with the E-mail Policy.

Protection of Network Transmissions.
In order to prevent unauthorized external access to electronic information transmitted over Revenue Analytics' electronic communications network, the IT Department shall implement the following procedures:

a. Access Configuration and Firewalls. To limit only authorized external access, the IT Department shall create and document a standard configuration for all servers, modems, routers, or other external access devices in accordance with the Access Control Policy.

b. Unauthorized Devices. Users shall not attach to the network unauthorized modems or other communications devices. The IT Department shall audit workstations and servers for unauthorized devices.
c. Remote Access Procedures. The IT Department shall allow users to connect remotely to on premise and cloud servers only by a secure socket layer (SSL) virtual private network (VPN) as provided to them by IT. Users are responsible for giving their remote access connection the same consideration and protection as Users give their onsite connection.
d. Users are responsible for any unauthorized use or for any breaches of security resulting from Users' remote access capability and may be subject to discipline up to and including termination.

Addressable Implementation Specifications.
The IT Department shall implement security measures to ensure that electronically transmitted information is not improperly modified without detection until disposed of.

a. One of these security measures shall be to use an SSL connection for electronic information received via Revenue Analytics' website that provides integrity of communications along with authentication using digital certificates.
b. Management shall require clients to use an SSL connection that provides integrity of communications, along with two-factor authentication using digital certificates, if Revenue Analytics will transmit or access electronic information via the client's website.

Revenue Analytics has determined that it is appropriate to implement encryption on electronic information received via Revenue Analytics' website. The IT Department shall ensure that SSL encryption is used on any web page in which electronic information may be entered or received. However, Revenue Analytics has determined that it is not appropriate to encrypt all electronic information transmitted via open networks due to the absence of any standard in this area, the difficulty in communicating with clients, providers, and payors. Management shall review this determination on an annual basis to determine if it is still not appropriate to implement encryption on all transmissions containing electronic information over an open network.