



Audit Reporting Auto Pilot Policies and Procedures

Policies and Procedures - Audit Reporting Auto Pilot (“R.A.P.”)

1.1 Data Protection, Data Storage, and Disposal

During the time we provide the R.A.P. service, Audit Software Professionals (“ASP”) will adhere to self-imposed policies governing data protection, data storage, and disposal.

1.1.1 ADT Security

ASP will store process and store client data in their individual office locations. Rich Lanza and Scott Gilbert both have security systems to protect all data and hardware used to provide the R.A.P. service.

1.1.2 PC Passwords

All work is performed on the partners’ individual PCs, which are password protected to prevent unauthorized access. No client data is stored on these PCs but rather on external harddrives (see section 1.1.3). These PCs will be stored at an ASP partner’s office.

ASP has implemented the following guidelines for PC passwords that all ASP partners and employees must follow:

Password Policies:

- Passwords must be changed every 6 months.
- Password uniqueness is set to remember 6 passwords that can not be reused.
- Users will be notified 2 weeks in advance of password expiration date. At this time, users will be prompted to select a new password.
- All passwords must conform to the guidelines outlined below.

Password Creation Guidelines

- Passwords are used to access any number of company systems, including the network, e-mail, the MRP, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.
- Passwords should not be based on well-known or easily accessible personal information.
- Passwords must contain at least 6 characters.
- Passwords must contain uppercase letters, lowercase letters and some numerical characters.

Password Protection Guidelines



Audit Reporting Auto Pilot Policies and Procedures

- Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person, including ASP partners, administrators, superiors, other co-workers, friends, and family members, under any circumstances.
- If someone demands your password, have them contact an ASP partner.
- Passwords are not to be transmitted electronically over the unprotected Internet, such as e-forms and/or via e-mail.
- No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.
- Do not use the “Remember Password” feature of any applications.
- Passwords used to gain access to company systems should not be used as passwords to access non-company accounts or information.
- If possible, don’t use the same password to access multiple company systems.
- If an employee either knows or suspects that his/her password has been compromised, it must be reported to an ASP partner and the password changed immediately.

1.1.3 External Hard Drives with Encryption

As an extra layer of protection, ASP uses encrypted hard drives to further protect the integrity of all client data. No client data will be accessible to anyone, except for ASP’s partners, employees, or subcontractors. The encrypted hard drives are password protected and will only be accessible by ASP partners. If an unauthorized individual tries to access the encrypted hard drive, the data will be unreadable.

1.1.4 Non-Disclosure Agreement

All clients will be required to sign a non-disclosure agreement with ASP. As a policy, ASP shall instruct its agents and employees and any subcontractors to treat all customer’s professional or business information, including but not limited to, data or information related to the customer's business, its clients, information supplied by its clients, marketing plans, sales, personnel, pricing policies, operational methods, business methods, trade secrets, “know how”, technical processes, inventions and research projects, and any other information designated by the customer as confidential or proprietary (“Confidential Information”), as confidential and shall not disclose the Confidential Information to other persons except as is reasonably necessary in connection with furnishing the services required under this Agreement and after having obtained the written consent of the customer. ASP shall not use any



Audit Reporting Auto Pilot Policies and Procedures

Confidential Information for any purpose except the provisions of services to the customer or its customers as set forth in this Agreement.

The terms, conditions and schedules of this Agreement shall remain confidential between the customer and ASP, and ASP shall not provide a copy of this Agreement, or disclose the terms thereof, to any third party without the prior written consent of the customer.

1.1.5 Delete Data After Engagement

As a policy, ASP partners and employees will delete all client data from ASP's storage devices and hard drives after ASP has completed each client engagement. No client data will be retained, unless specifically requested by a client.

1.2 Client Responsibilities and ASP's Responsibilities

During the time we provide the R.A.P. service, ASP and the client will have specific responsibilities to perform while engaged in the project.

1.2.1 Client Responsibilities

The client will be responsible for the following:

- Data Acquisition and Assessment: The client will be required to provide all necessary data for ASP to perform their data analysis. ASP will work with the client to identify the files and fields required for the analysis. ASP will work with the client to finalize the data formats required for ASP to perform the R.A.P. services.
- Data File Formats: The client will provide, upon request, data file layouts for all files provided to ASP. The file layouts will include the data field name, data field type, and field length.
- Answers to Data Questions: The client, upon request, will provide any necessary information to ASP or answer any data questions to help ASP prepare the data analysis reports. ASP will provide these data questions to the client as part of the audit data request.
- Client Data Validation: The client will be responsible for providing ASP with all necessary controls reports to help ASP verify with the client that the data provided to ASP is accurate and complete.

1.2.2 ASP Responsibilities

ASP will be responsible for the following:



Audit Reporting Auto Pilot Policies and Procedures

- Project Scoping: ASP will work with the client to scope out the details of the R.A.P. project specific for the client's needs. ASP will provide the client with an overview of the procedures ASP will perform and deliverables ASP will provide to the client. As part of this process ASP will outline the data required to be analyzed for the R.A.P. service.
- Data Request: ASP will provide each client with a detailed data request for information required for ASP to deliver R.A.P. services. This data request will outline specific data fields, including data types and lengths for all required files.

Additionally, ASP will provide the client with some questions for them to answer regarding details essential for ASP to provide the necessary data analysis. For example, ASP may ask the client for General Ledger approval limits.

ASP will request that clients provide data on a CD, DVD, or similar media.

- Data Receipt and Validation Tests: ASP will work with the client to ensure all data is validated prior to providing the R.A.P. service. This will include requesting any necessary reports.

Once ASP receives the required data from the client, ASP will perform validation tests by obtaining record counts and control totals from the client to assure the completeness and accuracy of the data ASP receives. ASP will generate totals for all numeric fields from the files provided by the client. ASP will compare the totals for those fields to the control totals provided by the client.

ASP will also perform some data relevance tests on the client files provided to verify that all data fields reflect the correct information as indicated in the file layout.

ASP will assess the relevance of the data ASP receives by requesting table explanations and field definitions from the client and by comparing file totals to reports produced by the client during the normal course of business. We will work with data mining/analysis tools to normal the data, if necessary.

- Report Execution: ASP will develop and run all data analysis reports, required to deliver the R.A.P. service. Reports will be developed using specific data mining, including but not limited to ACL, ActiveData for Excel, MS Excel, and MS Access. Reports will be limited based on the actual data provided by the client in that if all data per the data request is not provided, not all of the desired reports will be executed for the client.
- Provide Results to Client: ASP will provide the client with easy-to-follow analysis reports in Microsoft Excel, Access, and/or Word. ASP will



Audit Reporting Auto Pilot Policies and Procedures

provide all data analysis reports to the client in electronic formats. Deliverables will include detailed documentation of test performed and audit work to perform with the results. ASP will review the final data analysis reports with the client and present their findings.

- Additional Roles and Responsibilities: ASP professionals will also be responsible for the following tasks for each data analysis project:
 - Strategy Development and Quality Control
 - Project Management

1.3 Data Transfer Procedures

1.3.1. Mailing addresses for CDs

Once a client has engaged ASP to perform R.A.P. services, they will be required to provide data on a CD or similar media to ASP.

1.3.2. Ibackup policies and procedures

As a standard operating procedure, ASP will transmit and store all sensitive client data using the Ibackup service (www.ibackup.com).

Backup Procedures

ASP will adhere to the following procedures to properly backup all client data and R.A.P. related programs:

- All external hard drives where client data are stored have secondary copies of data on the IBackup service which will serve as a secure off-site backup of all client data and related data analysis.
- ASP will perform FULL backups of client data and related data analysis (R.A.P.) programs on a weekly basis on Fridays after normal business hours (after 5:00 p.m.)
- Weekly backups will be retained for 1 year, after which they will be deleted. Please note that data will be deleted earlier to one year if requested by the client.