Third Party Intake Form	Response	Third Party's Response to APS Comments/Questions
Do you have an existing contract with APS?	No	
If so,		N/A
What is the duration of the contract? Please provide date range in comments		N/A
Please provide a brief description of the project or service		N/A
Please provide all applicable project numbers		N/A
Do you have any subsidiary companies or do any business under any other names, that may be contracted with APS? If so, list in comments	No	
Third Party Risk Review Questionnaire	**Response**	**Third Party's Response to APS Comments/Questions**
Policy Verification (Please provide items listed below when submitting this completed questionnaire)		
Please provide the following documentation to APS, along with this completed questionnaire: Answer NO in the response column if you do not have these items		
Information Security Policy - Table of Contents and Revision History pages will suffice	Yes	
Most recent 3rd party attestation report, i.e. SSAE 16 SOC 1 or SOC 2, ISO certificate	No	
Data Types		
Do you obtain sensitive data from APS? Please list all that apply. APS considers the following as sensitive data, but is not limited to :	No	
HIPAA - “Individually identifiable health information including demographic data, that relates to the individual’s physical or mental health or condition, the provision of health care to the individual, or payment for the provision of health care to the individual."		N/A
PII -"Personally identifiable information (PII), is information that can be used on its own or with other information to identify, contact, or locate an individual."		N/A
PCI - "Peripheral Component Interconnect is an interconnection system between a microprocessor and attached devices."		N/A
SOX - "Data of the nature which contributes to or is included in regulatory required financial reporting for companies in scope of the Sarbanes-Oxley Act (Pub.L. 107–204)".		N/A
NERC-CIP - "North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the assets required for operating		N/A
NRC 10 CFR 73.54 - "Protection of digital computer and communication systems and networks related to Nuclear Plants"		N/A
10 CFR 810 - "Technology or technical information for the development, production or use of equipment or material especially designed or prepared for any of the listed activities, which includes nuclear reactor development, production or use of the components within or attached directly to the reactor vessel, the equipment that controls the level of power in the core, and the equipment or components that normally contain or come in direct contact with or control the primary coolant of the reactor core.”		N/A
15 CFR 774 - "The Commerce Control List (CCL) includes commodities, software, and technology subject to the authority of the U.S. Bureau of Industry and Security (BIS)		N/A
22 CFR 120-130 - "Defense articles and defense services in scope under the International Traffic in ARMS Regulations (ITAR)"		N/A
Is Customer data, Employee data or Contractor data being obtained?	No	
Other data obtained from APS, not listed above?	No	
How will information be transmitted from APS to vendor?		N/A
Human Resources & Employee Training		
Does the company perform any of the following background checks:	Yes	
Past employment verification?	Yes	
Criminal history?	Yes	
Credit history?	No	
Does the company perform Information Security awareness training for current and new employees?	Yes	
If yes, how often is this training received?	Yes	annually
If yes, are contractors and other external third-party contractors provided with the training?	Yes	
Does the company maintain a standards of business conduct/ethics policy?	Yes	
Does the company maintain a business conduct hotline for employees to report issues?	No	
Does the company provide privacy awareness training for employees and contractors?	Yes	
Is there a process or policy in place for employee termination or job transfer that immediately protects unauthorized access to information?	Yes	
Information Security		
Do you have a team within your organization dedicated to information security duties?	No	
If yes, how many full time employees does your Information Security Team consist of?	No	
Does the organization have written information security policies?	Yes	
If yes, please provide pages requested at row 4 of this questionnaire when responding to this assessment.		Row 4 does not apply
If yes, are security roles and responsibilities of constituents defined in accordance with the information security policy?	Yes	
Is role-based access utilized?	Yes	

If yes, describe.	Yes	GPA uses best practice security procedures including role based access to all GPA IT Infrastructure
Is least-privilege access control applied to user roles?	Yes	
Are entitlement changes including new access and terminations logged for audit purposes?	Yes	
Do third party vendors have access to your systems and data?	No	
If yes, describe		N/A
Does the organization outsource its data storage?	No	
If yes, to whom is the data outsourced and where are the servers that store the data located?		N/A
Is data encrypted in transit?		N/A
If yes, describe		N/A
Is data encrypted at rest?		N/A
If yes, describe		N/A
Physical Security		
Is there a physical security program?	Yes	
Is access to the operations floor restricted?	Yes	
Is physical access to the data center restricted?	Yes	
Is the physical access restricted with multifactor authentication?	Yes	
Are environmental controls present within the data center?	Yes	
Do external parties have unescorted access to systems and/or data processing facilities?	No	
If yes, describe		N/A
Do you retain records of who has accessed the data center?	Yes	
Do data centers have video monitoring?	No	
Change Management / Patch Management		
Is there change a management / change control policy or program in place?	Yes	
Is application development performed?	Yes	
If yes, is there a formal System Development Life Cycle process?	Yes	
Are system and security patches applied to workstations on a monthly basis?	Yes	
If no, how often?		weekly
Are system and security patches applied to servers on a quarterly basis?	Yes	
If no, how often?		monthly
Are system and security patches tested in a non-production environment prior to implementation in the production environment?	Yes	
Network Security		
Is antivirus / anti-malware software installed and maintained to the latest version on data processing servers?		N/A GPA has no data processing servers
If yes, which product?		
Is antivirus / anti-malware software installed and maintained to the latest version on workstations?	Yes	
If yes, which product?		Windows Defender
Do employees have a unique login ID when accessing data?	Yes	
Are passwords required to access systems containing APS data?		N/A GPA will not have access to APS Data
If yes, what is the required complexity and length for passwords?		N/A GPA will not have access to APS Data
Is there a process for secure disposal of both IT equipment and media?	Yes	
Are network boundaries protected by firewalls?	Yes	
Is regular network vulnerability scanning performed?	Yes	
Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization?	No	
If yes, How often are the rules updated and maintained?		N/A
Describe your remote access security controls		Remote Access is based on best practice including Certificate based access
Systems Security		
Is there formal control of access to System Administrator privileges?	Yes	
Are servers configured to capture who accessed a system and what changes were made?	Yes	
If no, in case of a security breach, how do you determine who accessed the system and what changes were made?		N/A
Business Continuity/Disaster Recovery		
Does the organization have a documented disaster recovery plan?	Yes	
If yes, is this planned, reviewed, and updated at least annually?	Yes	
If yes, is the disaster recovery plan tested?	No	
Is there insurance coverage for business interruptions or general services interruption?	Yes	
Have cross-functional dependencies been identified, as to determine how the failure in one system may negatively impact another one?	Yes	

Are there written backup procedures and processes in place?	Yes	
Are computer systems (servers) backed up on a regular schedule?	Yes	
If yes, what are the frequency of backups?		daily
Are backups periodically restored to ensure integrity of the backup?	Yes	
Does the organization store backups offsite?	No	
If yes, are backups encrypted?		N/A
Incident Response		
Is there a documented response program to address privacy incidents, unauthorized disclosure, or other unauthorized data access?	Yes	
If yes, will APS be notified within 24-36 hours?	Yes	
Does the organization have a formal Incident Response plan?	Yes	
Has the organization experienced an information security breach in the past?	No	
If so, how has your control environment matured as a result of the incident?		N/A
Do you have an incident response vendor on retainer in the event of an incident?	No	
Auditing / Client Reporting		
Is there an internal audit, risk management, or compliance function responsible for identifying and managing resolution of outstanding regulatory issues?	Yes	
Do you monitor the application and file logs for auditing?	No	The application is hosted by APS. GPA does not have access to the application.
Do you have the ability to see what was changed, who changed it, and when with the logs and audit files received?	No	The application is hosted by APS. GPA does not have access to the application.
Do you incorporate privileged access management within you network to servers, systems, applications, or files?	Yes	
Is the SysAdmin role enabled on your databases?	No	The application and database is hosted by APS. GPA does not have access to the database.
Data Privacy		
Is there a dedicated person or group responsible for privacy compliance?	Yes	
If yes, describe.		
Do you subcontract any services that would require you to share APS data with a third party?	No	GPA does not have access to APS data.
If yes, what service do you outsource to a third party?		N/A
If yes, who is the third party?		N/A
If yes, where is the third party's data center located?		N/A
If yes, is the third party monitored for privacy compliance?		N/A
Is there a removable media policy in place?	Yes	
In the event of relationship termination, are you able to delete APS specific data?	Yes	GPA does not have access to APS data.
Is personal information transmitted to countries outside of the United States?	No	
If yes, identify countries.		N/A
Does the organization store or replicate data to locations outside of the United States?	No	
If yes, identify countries.		N/A
Do you have a documented privacy policy?	Yes	No Information is shared with GPA
Are employees regularly monitored for privacy compliance?	Yes	
Do you have a process for responding to privacy complaints?	Yes	
Do you have a data retention policy?	Yes	We do not retain any data from APS
Is there a business process in place to ensure that information is used only for the purposes outlined in the agreement?	Yes	
Cloud Services		
Is this a cloud service? If no, this questionnaire is complete. If yes, continue answering the questions below	No	
What type [SaaS; PaaS, IaaS, Private Cloud, Public cloud, Community cloud, Hybrid cloud]		
Can APS define where data can be transmitted and stored?		
Where is the data center located?		
Are tenants isolated from each other?		
Is your cloud service encrypted?		
Are clients encryption keys ever shared?		
Can clients generate a unique encryption key?		
Can encryption keys be rotated on a scheduled basis?		
Is single sign-on utilized for this application?		
If not, what are your account administration policies?		
Is there a cloud audit program to address client audit and assessment requirements?		
If yes, please describe		
Are successful and unsuccessful last login attempts maintained for audit purposes?		
Do you have a process to notify clients, prior to changes being made, which may impact their service?		

Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other client's data?		
Will there be any email communication associated with the service?		
If yes, could the email coming from the client be interpreted as a piece of spoof email?		