Third Party Intake Form	Response	Third Party's Response to APS Comments/Questions	
Do you have an existing contract with APS?	No		
If so,	140	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" 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,		N/A	
which includes nuclear reactor development, production or use of equipment or material especially designed or prepared for any of the instead activities, which includes nuclear reactor development, production or use of the components within or attached directly to the reactor vessel, the equipment 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	N/A	
Is Customer data, Employee data of Colinacion data being obtained: Other data obtained from APS, not listed above?	No		
How will information be transmitted from APS to vendor?	110	N/A	
Human Resources & Employee Training	1	INA	
	Yes	T	
Does the company perform any of the following background checks: 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, now 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 mamata in 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, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes Yes		_		
			CDA hard dia a consider a consideration in a la dia a	
Name Provider secons counted galled so were rober? Ver	If yes, describe	Vac		
Acc antificient changes including own access and terminative logged for mailt purpose? New Year			Tole based access to an GLATT initiastructure	
No. 10 April 1974 Asserting the same state as your grown and dard? No.				
Systematics				
Date shee regularishen actionance in their stantage? No. No.			N/A	
Fryes, when is the data encorated and where are the server that store do located? NA NA NA NA NA NA NA N		No		
is us an expose in mana?** NA (Is days expressed at east? NA (Is days expressed at east?) NA (Is deep a point all sensity program? Yes (Is deep all sensity program? Yes (Is deex			N/A	
Seal or completed at core Physical Security Physical Securi			N/A	
Physical Security program Se	If yes, describe		N/A	
House a physical security arrayment (a teacher securities) (a security arrayment) (be secured that presentions) their extentional? (be security arrayment) (be secured that presentions) (be securities) (be security arrayment) (be security) (be	Is data encrypted at rest?		N/A	
Letter a physical security program? Security in the propriet access to the data center restricted? 1 spysical access to the data center? 1 spysical access to the subject of the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject accessed the data center? 1 spysical access to the subject access to the subject accessed to the subject access	If yes, describe		N/A	
Secons to the operations floor restricted? Yes February Proposition of the data center restricted? Yes February Proposition secons restricted with multifactor authentication? Yes February Proposition secons restricted with multifactor authentication? Yes February Yes February Yes February Yes February Yes February Yes February Yes Yes February Yes Yes February Yes Yes February Yes Yes February Yes February Yes	Physical Security			
Secons to the operations floor restricted? Yes February Proposition of the data center restricted? Yes February Proposition secons restricted with multifactor authentication? Yes February Proposition secons restricted with multifactor authentication? Yes February Yes February Yes February Yes February Yes February Yes February Yes Yes February Yes Yes February Yes Yes February Yes Yes February Yes February Yes	Is there a physical security program?	Yes		
Section Physical access restricted with multifactor authentications? Yes Content of the post of the data center? Yes Content of the post of the processing facilities? Yes Content of the post of the processing facilities? Yes Content of the post of the processing facilities? Yes Content of the post of the post of the processing facilities? Yes Content of the post of the po	Is access to the operations floor restricted?	Yes		
Mes continuemental controls process within the data center? No	Is physical access to the data center restricted?	Yes		
Designating parties have unsecured access to systems and/or data processing facilities?	Is the physical access restricted with multifactor authentication?	Yes		
Fig. 6, describe Comparison of who has accessed the data center? Change Management / Patch Management	Are environmental controls present within the data center?	Yes		
Do you retain records of who has accessed the data center? No Do data centers have video monitoring? No Do data centers have video video monitoring? No Do data centers have video video monitoring? No Do data centers have video video m	Do external parties have unescorted access to systems and/or data processing facilities?	No		
Decidence (nearly have video monitoring? No Change Management / Patch Management	If yes, describe		N/A	
Change Management / Patch Management is there change a management / change control policy or program in place? is policiation 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 offen? New offen.	Do you retain records of who has accessed the data center?	Yes		
In the change a management / change control policy or program in place? In publication development performed? In publication development performed by a weekly In publication development performed? In publicati	Do data centers have video monitoring?	No		
Is application development performed? If yes, is there a formal System Development Life Cycle process? Are system and security patches applied to workstations on a monthly basis? If no. how other? Are system and security patches applied to servers on a quarterly basis? If no. how other? Are system and security patches paplied to servers on a quarterly basis? If no. how other? Are system and security patches tested in a non-production environment prior to implementation in the production environment? **Entwork Security** **Entwork Secu	Change Management / Patch Management			
Is application development performed? If yes, is there a formal System Development Life Cycle process? Are system and security patches applied to workstations on a monthly basis? If no. how other? Are system and security patches applied to servers on a quarterly basis? If no. how other? Are system and security patches paplied to servers on a quarterly basis? If no. how other? Are system and security patches tested in a non-production environment prior to implementation in the production environment? **Entwork Security** **Entwork Secu	Is there change a management / change control policy or program in place?	Yes		
As system and security patches applied to workstations on a monthly basis? 17 no. how ofher? As expstem and security patches applied to severe on a quarterly basis? 17 no. how ofher? As expstem and security patches sested in a non-production environment prior to implementation in the production environment? 18 antiviras' anti-malware software installed and maintained to the latest version on data processing servers? 19 sea, which product? 20 sea a unique login ID when accessing data? 21 sea, which product? 22 sea, which product? 23 sea, which product? 24 sea process for secure disposal of both IT equipment and media? 25 sea, process for secure disposal of both IT equipment and media? 26 sea, process for secure disposal of both IT equipment and media? 28 sequent network vulnorability seaming performed? 29 sequent network vulnorability seaming performed? 29 sequent network vulnorability seaming performed? 20 sea for secure disposal of both IT equipment and media? 29 sequent network vulnorability seaming performed? 20 sea for secure disposal of both IT equipment and media? 20 sea for secure disposal of both IT equipment and media? 20 sea for secure disposal of both IT equipment and media? 20 sea for secure disposal of both IT equipment and media? 20 sea for secure disposal of both IT equipment and media? 20 sea for secure disposal of both IT equipment and media? 21 sea for secure disposal of both IT equipment and media? 22 sea for secure disposal of both IT equipment and media? 23 sequent secure disposal of both IT equipment and media? 24 sea for secure disposal of both IT equipment and media? 25 sequent secure disposal of both IT equ		Yes		
Fin., how often?	If yes, is there a formal System Development Life Cycle process?	Yes		
Ace system and security patches applied to servers on a quarterly basis? 1 monthly 1	Are system and security patches applied to workstations on a monthly basis?	Yes		
If no, how often? Resystem and security patches tested in a non-production environment prior to implementation in the production environment? Resultivirus / anti-malware software installed and maintained to the latest version on data processing servers? If yes, which product? If yes, which are a unique login ID when accessing data? Are passwords required to access systems containing APS data? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what when the product with the product of the pro	If no, how often?		weekly	
Ace system and security patches tested in a non-production environment prior to implementation in the production environment? Network Security Network Security Santivinus / anti-malware software installed and maintained to the latest version on data processing servers? If yes, which product? Is antivinus / anti-malware software installed and maintained to the latest version on workstations? If yes, which product? Is antivinus / anti-malware software installed and maintained to the latest version on workstations? If yes, which product? In yes, what is the required to access systems containing APS data? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, length enter the rules updated and maintained? Yes If yes, length enter the rules updated and maintained? If yes, length enter the rules updated and maintained? If yes, length enter the rules updated and maintained? If yes, if the jaccess the security reach, bow doy out determine who accessed the system and what changes were made? If yes If yes, if his planned, reviewed, and updated at least annually? Yes If yes, is the planned, reviewed, and updated at least annually? If yes, is the planned, reviewed, and updated at least annually? If yes, is the flasses the flasses the force increption? Yes If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery	Are system and security patches applied to servers on a quarterly basis?	Yes		
Season S	If no, how often?		monthly	
is antivirus / anti-malware software installed and maintained to the latest version on data processing servers? If yes, which product? If yes, which product yes yes yes yes which products yet yes	Are system and security patches tested in a non-production environment prior to implementation in the production environment?	Yes		
If yes, which product? If yes, which great required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes a process for secure disposal of both IT equipment and media? Are network boundaries protected by firewalls? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, what is the required complexity and length for passwords? If yes, is the jean the volument of access to System Administrator privileges? If yes, is the jean the volument of access to System Administrator privileges? If yes, is this planned, reviewed, and updated at least annually? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? If yes, is the islanter covery plan tested? If yes the islanter covery plan tested? If yes the islanter covery plan tested? If yes the islanter covery pl	Network Security			
Santiviras / anti-malware software installed and maintained to the latest version on workstations? Yes Windows Defender			N/A GPA has no data processing servers	
If yes, which product? Do employees have a unique login ID when accessing data? Are passwords required to access systems containing APS data? If yes, what is the required complexity and length for passwords? Is there a process for secure disposal of both IT equipment and media? Are network boundaries protected by firewalls? Is regular network vulnerability scanning performed? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? If yes, How often are the rules updated and maintained? Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruption or general services interruption? Are services configured to apture who accessed a system and what changes were made? Yes If yes, is the insurance coverage for business interruption or general services interruption? Are serviced to specify because the system and what changes were made? Yes If yes, is the insurance coverage for business interruption or general services interruption? Yes If yes, is the insurance coverage for business interruption or general services interruption? Yes If yes, is the insurance coverage for business interruption or general services interruption? Yes Is there insurance coverage for business interruption or general services interruption? Yes If yes, is the disaster recovery plan tested? Yes If yes, is the disaster recovery plan tested? Yes If yes, is the disaster recovery plan tested? Yes If yes, is the disaster recovery plan tested? Yes If yes, is the disaster recovery plan tested? Yes If yes If yes, is the disaster recovery plan tested?				
Do employees have a unique login ID when accessing data? Are passwords required to access systems containing APS data? Are passwords required to access systems containing APS data? If yes, what is the required complexity and length for passwords? Is there a process for secure disposal of both IT equipment and media? Are network boundaries protected by firewalls? Are network whencability scanning performed? Are lattusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? If yes, How often are the rules updated and maintained? Systems Security Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, nease of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan lested? Yes If there insurance coverage for business interruptions or general services interruption? Yes If the insurance coverage for business interruptions or general services interruption?		Yes		
Are passwords required to access systems containing APS data? If yes, what is the required complexity and length for passwords? Are network boundaries protected by firewalls? Are network boundaries protected by firewalls? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are server security controls Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? Are servers configured to capture who accessed a system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is this planned, reviewed, and updated at least annually? Is there insurance coverage for business interruptions or general services interruption? Yes Is the insurance coverage for business interruptions or general services interruption?			Windows Defender	
If yes, what is the required complexity and length for passwords? Is there a process for secure disposal of both IT equipment and media? Are network boundaries protected by firewalls? Is regular network vulnerability scanning performed? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? If yes, How often are the rules updated and maintained? Systems Security Bescribe your remote access security controls Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the finance coverage for business interruptions or general services interruption? Yes Is there insurance coverage for business interruptions or general services interruption? Yes Is the required cispose of the System Administrator privileges and what changes were made? Yes If yes, is this planned, reviewed, and updated at least annually? Yes If yes, is the insurance coverage for business interruptions or general services interruption? Yes		Yes		
Is there a process for secure disposal of both IT equipment and media? Are network boundaries protected by firewalls? Are network boundaries protected by firewalls? Are protected by firewalls? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? Are Systems Security controls Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security beach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes If yes, is this planned, reviewed, and updated at least annually? Is the insurance coverage for business interruptions or general services interruption?				
Are network boundaries protected by firewalls? Is regular network vulnerability scanning performed? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? If yes, How often are the rules updated and maintained? Systems Security Systems Security Systems Security Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? Is the disaster recovery plan tested? Is the insurance coverage for business interruptions or general services interruption? Yes Is the insurance coverage for business interruptions or general services interruption?			N/A GPA will not have access to APS Data	
Is regular network vulnerability scanning performed? Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? If yes, How often are the rules updated and maintained? Describe your remote access security controls Systems Security Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is their disaster recovery plan tested? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery for business interruptions or general services interruption? Yes Is there insurance coverage for business interruptions or general services interruption?				
Are Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) used by your organization? If yes, How often are the rules updated and maintained? Describe your remote access security controls Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? No Remote Access is based on best practice including Certificate based access No No Remote Access is based on best practice including Certificate based access No Remote Access is based on best practice including Certificate based access No Remote Access is based on best practice including Certificate based access No No Is there formal control of access to System Administrator privileges? Yes If yes, is the formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? Yes Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access to System Administrator privileges? No Is there formal control of access				
If yes, How often are the rules updated and maintained? Remote Access is based on best practice including Certificate based access Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? N/A Remote Access is based on best practice including Certificate based access N/A Remote Access is based on best practice including Certificate based access Yes Yes N/A Yes If yes, is the identificate based access N/A If yes, is the identificate based access No If yes, is the identificate based access No Is there insurance coverage for business interruptions or general services interruption?				
Describe your remote access security controls Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Remote Access is based on best practice including Certificate based access Yes Remote Access is based on best practice including Certificate based access Certificate based access Aves		No	27/1	
Describe your remote access security controls Systems Security Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Certificate based access Yes Maccessed access No	If yes, How often are the rules updated and maintained?			
Is there formal control of access to System Administrator privileges? Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes If yes Yes If yes, is the disaster recovery plan tested? Yes Yes Yes If yes, is the disaster recovery plan tested? Yes Yes	Describe your remote access security controls			
Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes Yes Yes If yes, is the disaster recovery plan tested? No Is there insurance coverage for business interruptions or general services interruption? Yes	Systems Security	·		
Are servers configured to capture who accessed a system and what changes were made? If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes Yes Yes If yes, is the disaster recovery plan tested? No Is there insurance coverage for business interruptions or general services interruption? Yes	Is there formal control of access to System Administrator privileges?	Yes		
If no, in case of a security breach, how do you determine who accessed the system and what changes were made? Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? No Is there insurance coverage for business interruptions or general services interruption? Yes				
Business Continuity/Disaster Recovery Does the organization have a documented disaster recovery plan? If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes			N/A	
If yes, is this planned, reviewed, and updated at least annually? If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes Yes				
If yes, is the disaster recovery plan tested? Is there insurance coverage for business interruptions or general services interruption? Yes	Does the organization have a documented disaster recovery plan?	Yes		
Is there insurance coverage for business interruptions or general services interruption? Yes	If yes, is this planned, reviewed, and updated at least annually?	Yes		
	If yes, is the disaster recovery plan tested?	No		
Have cross-functional dependencies been identified, as to determine how the failure in one system may negatively impact another one?				
	Have cross-functional dependencies been identified, as to determine how the failure in one system may negatively impact another one?	Yes		

		I
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 information security breach in the past?	No	
If so, how has your control environment matured as a result of the incident?	110	N/A
Do you have an incident response vendor on retainer in the event of an incident?	No	1071
	110	
Auditing / Client Reporting		
Is there an internal audit, risk management, or compliance function responsible for identifying and managing resolution of outstanding regulatory issues?	Yes	
		The application is hosted by APS. GPA does not
Do you monitor the application and file logs for auditing?	No	have access to the application.
		The application is hosted by APS. GPA does not
Do you have the ability to see what was changed, who changed it, and when with the logs and audit files received?	No	have access to the application.
Do you incorporate privileged access management within you network to servers, systems, applications, or files?	Yes	
		The application and database is hosted by APS. GPA
Is the SysAdmin role enabled on your databases?	No	does not have access to the database.
Data Privacy		
Is there a dedicated person or group responsible for privacy compliance?	Yes	
Is unto a tectuated person of group responsible for privacy compinance. If we, describe.	103	
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?	110	N/A
If yes, what service do you doubsource to a direct party. 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	1011
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.	110	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?	