Attachment E: SLA's

2024-PRMP-MES-AVS-005

Turnover	Turnover and Closeout Management Plan defines the vendor's responsibilities related to turnover. Turnover will not be considered complete until the Turnover and Closeout Management Plan and its associated deliverables are accepted by PRMP.	PRMP shall assess up to $500 per calendar day for each day after the due date that an acceptable Turnover and Closeout Management Plan is not submitted. PRMP shall assess up to $500 per calendar day for each day after 30 calendar days from the date of the turnover of operations that the Turnover Results Report is not submitted
Turnover Documentation/ Data Handoff	The vendor must provide to PRMP or its designee, within seven (7) business days of notice of termination the following information: • Copies of all subcontracts and third-party contracts executed in connection with the services included in this contract. • A list of services provided by subcontractors, including the names and contact information for the subcontractors. • Other documentation as defined by PRMP, as evaluation materials, raw data, research information, and others.	PRMP shall assess up to $500 for each calendar day beyond the seven (7) business days that all required materials are not delivered by the vendor.
Bi-weekly Status Reports	The vendor must provide bi-weekly reports identifying the status of the activities, including any issues.	PRMP shall assess up to $200 per calendar day for each day an acceptable bi-weekly report is not timely received. If the report is received on time but the information reported is inaccurate or incomplete, PRMP shall assess up to $200 per day until an acceptable report is received.
Key Staff	During the entire duration of the contract, key staff commitments made by the vendor must not be changed without thirty (30) days prior written notice to PRMP unless due to legally required leave of absence, sickness, death,	Up to a maximum of $1,000 per occurrence shall be assessed for each key staff person proposed who is changed without proper notice and approved by PRMP for reasons other than legally required leave of absence,

	resignation, or mutually agreed-upon termination of employment of any named individual.	sickness, death, or termination of employment.
Key Staff Replacement	The vendor will replace key staff in a timely fashion. Replacement of key staff will take place within thirty (30) calendar days of removal unless a longer period is approved by PRMP's authorized representative.	PRMP shall assess up to $200 per business day for each business day after the initial thirty (30) calendar days allowed in which an acceptable replacement for that key staff position is not provided.
Email Triage and Acknowledgment	The vendor must triage all inquiries received from PRMP. All emails received must be acknowledged within twenty-four (24) hours of receipt and resolved within three (3) business days unless otherwise approved by PRMP. The vendor must forward to the designated PRMP staff within one (1) calendar day those inquiries that are either: 1. Determined to be outside the response scope for the vendor. 2. Should be handled by PRMP staff. Compliance and Calculation: • Acknowledge all emails received within twenty-four (24) hours and resolve all emails within three (3) business days. • Forward to PRMP staff within one (1) calendar day emails that are determined to be outside of the vendor's response scope.	$100 per occurrence of an email not being acknowledged within twentyfour (24) hours. $100 per occurrence of an email resolution not received within three (3) business days. $100 per occurrence of any emails forwarded to outside the response scope of the vendor within one (1) calendar day
Security breach	The vendor must establish and maintain systems, processes, and security features to protect beneficiary information from unauthorized access according to PRMP policies and procedures. Data related to Medicaid beneficiaries' demographic and personal health information (PHI)	The PRMP shall assess up to $500 for each beneficiary whose information is accessed without authorization and is attributable to a fault of the vendor, according to the PRMP policies and procedures. The PRMP shall assess up to $10,000 for each day that a security breach attributed to the vendor goes

	must not be breached (accessed without authorization)	unreported to PRMP after discovery of a security breach.
	The Security and Privacy Incident Notification Service Level is defined as the vendor's documented response approach/plan for handling any potential threats to data, data breaches, or privacy incidents as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The vendor should notify PRMP of any incidents or breaches. 1. Upon discovery, report confirmed incidents to PRMP. 2. Information security officer, privacy officer or designee confirms, quantifies, and categorizes suspected incidents within three business days. 3. Contain incident as soon as possible 4. Detailed incident report is submitted to PRMP within one business day of confirming incident. 5. Develop incident communication plan. 6. Briefing with PRMP within five (5) business days of incident confirmation. 7. Remediate the issue at hand and complete a full incident report.	The vendor shall compensate PRMP for any fines and penalties imposed by regulatory entities. PRMP may, at its discretion, withhold operating fee payments until fines and penalties are resolved.