Anexo Estándar - Requisitos de Seguridad de la Información (SI)

El Contratista acuerda maximizar la seguridad de sus personas, procesos y tecnologías a lo largo de la vigencia de este Contrato de conformidad con los requisitos establecidos en este Anexo y todas las leyes aplicables (colectivamente, los "**Requisitos de SI**"). La Compañía se reserva el derecho de validar la efectividad de los Requisitos de SI o el Contratista deberá proporcionar evidencia de una validación independiente por parte de un tercero, a solicitud de la Compañía. La Compañía podrá modificar los Requisitos de SI mediante notificación por escrito al Contratista. El término "producto", como se usa en este documento, significa cualquier servicio, equipo, sistema o software proporcionado por el Contratista a la Compañía en términos de este Contrato.

1. **Controles de Acceso**. El Contratista proporcionará controles de acceso, autorización y responsabilidad basados en roles dentro de su producto, que cumplan con las pautas y requisitos establecidos en los Requisitos de SI. Los controles deben ser apropiados para la sensibilidad de la información. Además, el producto proporcionará roles separados para los usuarios del día a día, administradores, desarrolladores y personal de soporte, y que el acceso, proporcionará acceso sólo al personal autorizado que haya recibido la capacitación adecuada sobre responsabilidades administrativas, procesos y procedimientos de seguridad. El control del acceso deberá proporcionar el acceso mínimo requerido para cada rol y denegará el acceso a usuarios no autorizados. Los productos alojados por el Contratista, si los hubiere, incluirán controles para proteger las cuentas de servicio y las cuentas genéricas, para evitar su modificación o uso no autorizado. Las contraseñas de las cuentas de servicio y las genéricas deben cambiarse al menos una vez al año. Adicionalmente, el Contratista también garantizará que los administradores del entorno de producción de los productos alojados utilizarán la autenticación de dos factores al proporcionar soporte administrativo remoto para el entorno.

2. **Arquitectura Compartida**. El Contratista acepta identificar las partes en donde los recursos compartidos sean utilizados dentro de su arquitectura por otros clientes y los controles de seguridad implementados para proteger los datos de la Compañía del acceso de usuarios no autorizados y de terceros. Si este Contrato considera un entorno dedicado, entonces dicho entorno no contendrá recursos compartidos, incluyendo, pero no limitándose a todos los componentes, sistemas e infraestructura.

3 **Respuesta a Incidentes y Notificación de Filtraciones**. El Contratista acuerda que cualquier filtración o cualquier otro incidente de seguridad, interno o externo, que pueda comprometer múltiples fuentes de datos, deberá informarse al Centro de Operaciones de Seguridad de la Compañía (soc@sempra.com (858) 613-3278) dentro de las 24 horas a partir del conocimiento de la filtración, seguido de un de plan de remediación de 72 horas, y 2 semanas hábiles a partir de la notificación inicial para completar la investigación.

4 **Cifrado**. Cuando la Compañía determine que el cifrado es aceptable para evitar la divulgación no autorizada de la información de la Compañía, para proteger la información sensible de la Compañía, los productos del Contratista usarán controles criptográficos que satisfacen los requisitos de FIPS 197 de tal manera que los datos e información sensible de la Compañía sean inaccesibles por un usuario no autorizado. Cuando el producto del Contratista utilice llaves de cifrado, el producto del Contratista no almacenará las llaves de cifrado dentro del código fuente. Las llaves de cifrado se almacenarán y protegerán por separado del producto mientras estén en tránsito y en reposo, y serán revocables para su reimplementación y mantenimiento.

5 **Estándares de Contraseñas y de Inicio de Sesión**. Los productos del contratista proporcionarán un identificador único (identificable individualmente) para las cuentas de usuarios. Cuando no se pueda lograr la responsabilidad individual para el acceso a sistemas sensibles, se deberá de emplear la autenticación de múltiples factores. Los productos del Contratista proporcionarán una complejidad de contraseña que cumpla con los siguientes parámetros: mínimo de 8 caracteres alfanuméricos, 90 días de antigüedad de la contraseña y el historial de 10 contraseñas anteriores. Las credenciales de inicio de sesión y las contraseñas estarán protegidas por un cifrado de transporte que cumpla con los requisitos mínimos de cifrado de la Sección 4.0.

6 **Seguridad de los datos**

a. Certificación de seguridad del producto. El Contratista certifica que su producto proporciona la seguridad necesaria para cumplir con todas las leyes y requisitos reglamentarios aplicables para el almacenamiento, el procesamiento y la transmisión de datos. Esto incluye específicamente, pero no se limita a, todas las leyes y reglamentos que requieren protecciones específicas para la información de identificación personal, información financiera y de tarjetas de crédito, y los registros de auditoría. El Contratista acepta en que permitirá la validación por parte de la Compañía o por terceros contratados por ella para verificar el cumplimiento de todos los requisitos legales y reglamentarios.

b. Capacidad de bloqueo/restricción. En caso de que se sospeche o se produzca una violación o compromiso sospechoso o real que involucre la infraestructura del Contratista, esté o no relacionada con el producto, la Compañía podrá, a su entera discreción, bloquear o restringir todos y cada uno de los métodos y fuentes de acceso del Contratista, incluyendo, sin limitación, la comunicación, la conectividad y las integraciones (colectivamente, "Derecho de bloqueo"). Sin perjuicio de cualquier otro requisito u obligación de la Compañía en el presente Contrato, si la Compañía ejerce su Derecho de Bloqueo, la Compañía no tendrá ninguna responsabilidad hacia el Contratista que surja o esté relacionada de alguna manera con el mismo. El acceso requerido del Contratista sólo se restablecerá después de que el Contratista haya demostrado efectivamente, a través de un tercero independiente y competente, que su producto y los sistemas relacionados ya no representan una amenaza potencial o real para la Compañía.

7 **Registro y Detalles de Errores**. El Contratista acepta registrar todo el uso de productos y aplicaciones, el acceso de los usuarios, el uso indebido y los mensajes de error detallados necesarios para monitorear y analizar el uso de los productos, y retendrá toda la información durante un mínimo de noventa (90) días a partir de la fecha de registro. El Contratista además acepta que el producto incluya una pista de auditoría, entradas de registro de tiempo, así como un identificador de registro único. La Compañía se reserva el derecho de solicitar los registros en cualquier momento y sin costo para la Compañía.

8 **Vulnerabilidades y Defectos**. El Contratista acepta mantener un proceso de seguimiento de vulnerabilidades y defectos que identifique los posibles defectos, además de clasificarlos por su impacto en la seguridad de los productos del Contratista y los componentes y paquetes de *software* que lo respaldan, sin costo alguno para la Compañía. El Contratista conviene también en que, a expensas del Contratista, probará y remediará todas las vulnerabilidades de *software* divulgadas públicamente en la Base de datos de vulnerabilidades de Estados Unidos (http://nvd.nist.gov/) y por Open Web Application Security Project (www.owasp.org) dentro de los treinta (30) días posteriores a su publicación. En general, esto evitará que el producto sea fácilmente susceptible a ataques de secuencias de comandos entre sitios, inyección SQL, desbordamientos de búfer,

validación de entradas y otros ataques similares. El Contratista garantiza además que el producto no contendrá ningún código que pueda facilitar el acceso inesperado o no aprobado o interrupciones del producto, incluidos, entre otros: virus informáticos, gusanos, bombas de tiempo, puertas traseras, caballos de Troya, huevos de pascua y cualesquiera otras formas de código malicioso, y acepta proporcionar documentación que detalle dichos procesos a solicitud de la Compañía y sin costo para la Compañía.

9 **Evaluaciones y Pruebas de Seguridad**. El Contratista acuerda que contratará a un tercero independiente, que será acordado por el Contratista y la Compañía, a expensas del Contratista, para probar el producto en busca de vulnerabilidades a través de una prueba de seguridad detallada anualmente, mediante una Certificación Estándar de la Industria (por ejemplo, ISO 27000, SOC2 Tipo 2, etc.). En lugar de una certificación Estándar de la Industria, el Contratista puede optar por realizar una prueba de seguridad anual de los controles de seguridad de la información que respaldan el producto, su entorno de alojamiento de producción y la infraestructura de soporte operativo. El Contratista deberá solicitar a dicho tercero que proporcione un informe que detalle los resultados de la prueba y el Contratista deberá proporcionar a la Compañía una copia de dicho informe dentro de los treinta (30) días posteriores a la prueba. En el caso de que dicho informe muestre vulnerabilidades en el producto, el Contratista deberá proporcionar de inmediato a la Compañía un plan de remediación propuesto y un cronograma para su finalización, todo sin costo para la Compañía. Todas las vulnerabilidades, defectos o errores del producto revelados al Contratista serán corregidos y remediados por el Contratista, a expensas del Contratista, dentro de los treinta (30) días a partir de la fecha de dicho informe.

10 **Derecho a Informar**. La Compañía y/o el Contratista tienen el derecho de informar a las organizaciones de base de datos de vulnerabilidades públicas sobre cualquier defecto o condición de configuración que resulte en vulnerabilidades a la información manejada por el producto mismo u otro hardware, software o sistemas que pudieran poner en riesgo a la Compañía y/o a los intereses de la Compañía.

11 **Destrucción**. El Contratista acepta que, cuando se haya superado el período de retención de los datos, cuando los datos ya no sean necesarios, o a petición de la Compañía, el Contratista destruirá los datos de una manera que los hará completamente inutilizables e irrecuperables, y proporcionarán a la Compañía un certificado de destrucción, a solicitud de la Compañía.

12 **Documentación Formal**. El Contratista acepta proporcionar documentación formal para el uso, mantenimiento e implementación segura del producto del Contratista. La documentación del producto se actualizará dentro de los treinta (30) días posteriores a la actualización, instalación de parches o cambio similar del producto. La documentación del producto incluirá, entre otras cosas, un inventario de todos los componentes, configuraciones y dependencias.

13 **Conflictos**. Nada de lo contenido en este Contrato se interpretará como una limitante de cualquiera de las obligaciones del Contratista en materia de no divulgación o protección de la información contenidas en otras partes de este Contrato, incluidos, entre otros, los términos y condiciones contenidos en el cuerpo principal del mismo.