R-04 DATA PROTECTION POLICY

Syntegra Technology, S. A., dedicated to:

"MARKETING AND PROFESSIONAL SERVICES OF ONLINE DATABASE MANAGEMENT SOFTWARE ."

During the execution of its activities and for the purpose of an adequate development **, Syntegra Technology accesses** and processes personal data of customers, collaborators, suppliers and other interested parties, whenever this processing is necessary to achieve the objectives of the organization.

The Management of Syntegra Technology, based on this processing of personal data, undertakes to comply with the data protection regulations that apply to it and, in particular, with the "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL" (RGPG), with Organic Law 3/2018 of December 5 on the Protection of Personal Data, and Law 81 of 2019 on the Protection of Personal Data in the Republic of Panama, which adapts the legal system to the aforementioned regulations.

Syntegra Technology's Management is aware of the Data Protection Policy, through which the organization undertakes to:

- Ensure the existence of a legal basis for the different processing of personal data, guaranteeing the lawfulness of these according to the cases set out in the regulations.
- Use the minimum data necessary to comply with the purposes indicated in each case, ensuring as far as possible the veracity and accuracy of these.
- Ensure compliance with the information with transparency (access, rectification, cancellation, opposition, portability and limitation of processing).
- Define and implement the necessary technical measures to ensure the confidentiality, integrity, availability and resilience of personal data. Taking into account in the context the techniques of nature, scope and risks
- Assume the commitment to minimise security breaches, as well as to collaborate with the Data Protection Agent supervisory authority (ANTAI-AIG), for the resolution of incidents or conflicts that may arise from non-compliance with regulations.
- Define the necessary and appropriate responsibilities to ensure compliance with the requirements of data protection regulations. Defining Policies Necessary Acceptable that are considered necessary.

This Policy will provide the reference framework for Syntegra Technology's compliance with data protection regulations, and is communicated to the entire Company and interested parties.

In order to comply with this Data Protection Policy, Syntegra Technology has implemented certain security procedures, measures and standards, as well as the definition of the Policies necessary to guarantee an adequate level of security in the processing of data and information.
In particular, users (collaborators) must be aware of and commit to comply with the following rules:

- The information assets (computer equipment, media, mobile devices, applications, etc.) belong to the Company, and their use must be used exclusively for work purposes, unless expressly authorised by the management. It is the responsibility of the user to take care of and treat the assigned computer and non-computer resources.
- Computer equipment has a default security setting. Users must not modify these configurations, nor install or download, without prior authorization, additional programs or software, and the use of software without the proper license, which may imply breaches of the Intellectual Property Law, is expressly prohibited.

- Illegal, obscene, immoral or offensive material or content that lacks the objectives of The Company, or that could violate morality or ethical standards, or that may infringe the rights of third parties may not be introduced into the systems or network or network.

- The user must maintain professional secrecy and maximum confidentiality in relation to the personal data to which they have access by virtue of their work, as well as any other information that they become aware of as a result of the activities they carry out in The Company. This obligation will continue even after your relationship with the data controller has ended.
- Files, lists or sets of personal data must not be created without the authorisation of the defined controllers, nor may they be communicated outside the Company without due authorisation.
- Users must ensure compliance with the principles and rights of data protection regulations. Ensuring compliance with the right to information when personal data is obtained.
- Exposure or possibility of access to unauthorised users of information and in particular personal data, through computer means, must be avoided as far as possible.
- As a general rule, users will only have access to the information they need to carry out their functions. It must be reported as an incident if it is detected that access to more information or more utilities than necessary is available.
- To control access to information, each user will have an individual name and password with specific access permission.
- Users are responsible for the use and custody of the access keys or passwords assigned to them. Under no circumstances should they be communicated to other users, nor should they be recorded or written in any format to avoid unauthorized access to them.
- The use by any user of the access and use of the permissions of other users is expressly prohibited. To install or modify applications on The Company's computers, impersonating the identity of another user.
- Similarly, it is expressly prohibited to attempt to increase the level of privileges of a user in the system, access resources without authorization, unauthorized use of passwords, deliberate exploitation of vulnerabilities and as well as attempt to distort or falsify the logs or records of the system.
- The user should only use corporate email for purposes related to the functions and tasks assigned to him/her. The user is responsible for all activities carried out under his/her email account. Which must not be used by unauthorized persons.
- It is the duty of the Company's employees to use the e-mail service appropriately and responsibly, in accordance with the good practices defined for this purpose: sending mass or large e-mails that may saturate the network, downloading unverified executables or attachments, sending unencrypted confidential data, use of corporate signature...
- The use of external media or other storage devices (pencils, USBs, hard drives,...) to store or transfer confidential information will require the express authorisation of those responsible or management.
- As a general rule, access to the Internet will be limited to purposes directly related to the activity of The Company and the tasks of the user's workplace. Users will not be able to access to download images, videos, illegal content or content contrary to morality and good customs.
- The Company may provide users with mobile devices for the performance of its functions. In which the information will be minimized as a general rule and its use will be limited to strictly professional purposes.
- With regard to the use of these BYOD elements, it will be ensured at least: the existence of antivirus systems, the correct updating of operating systems, avoiding physical access by unauthorized users, using logins or unique user accounts, or not storing information in them for longer than necessary.
- The Company reserves the right to review, without prior notice, the uses made of the information systems (access logs, e-mail messages, internet access,...) in order to check, prevent or react to vulnerabilities or security incidents, and ensure the integrity of the information systems.
- El usuario debe custodiar y velar por la protección del dispositivo móvil asignado. Con bloqueo automatic access, access via passwords or patterns, connection to known or secure wireless networks, authorization for installation of additional software, device encryption,...
- The backup of the information processed in The Company must be ensured , for which the appropriate procedures have been defined, making copies of the necessary directories, locations and systems. Users should ensure that the information they generate is in these directories, and that it is not only found on their own computers locally.

R-04 DATA PROTECTION POLICY

To learn more about the rules defined by the organization, the user must access the "**User Safety Guide**" that is included as an annex to this document. That it must be made available to all users with access to data, as well as to the rest of the Policies and Standards that have been defined and communicated by the organization. For public access to any interested party, the e-mail address contact@syntegracert.com is available.

The information security and data protection system covers all activities related to the marketing and professional services of online database management software.

Senior Management

Panama, April 1, 2026.

R-04 POLÍTICA DE PROTECCIÓN DE DATOS

Syntegra Technology, S. A., dedicada a:

"COMERCIALIZACIÓN Y SERVICIOS PROFESIONALES DE SOFTWARE DE GESTIÓN DE BASE DE DATOS EN LÍNEA."

Durante la ejecución de sus actividades y con la finalidad de un adecuado desarrollo **Syntegra Tecnology,** accede y trata datos de carácter personal de clientes, colaboradores, proveedores y otras partes interesadas., siempre que este tratamiento sea necesario para alcanzar los objetivos de la organización.

La Dirección de Syntegra Technology, en base a ese tratamiento de datos personales se compromete a cumplir con la normativa en materia de protección de datos que le sea de aplicación y, en particular, con el "REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO" (RGPG), con la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales, y la Ley 81 del 2019 de Protección de Datos Personales en la República de Panamá que adapta el ordenamiento jurídico a la citada normativa.

La Dirección de Syntegra Technology es consciente de la Política de Protección de Datos, mediante la cual la organización se compromete a:

- Asegurar la existencia de base jurídica para los diferentes tratamientos de los datos personales garantizando la licitud de estos según los supuestos recogidos en la normativa.
- Utilizar los datos mínimos necesarios para cumplir con las finalidades que se indiquen en cada caso asegurándose en la medida de lo posible de la veracidad y exactitud de estos.
- Asegurar el cumplimiento de la información con transparencia (acceso, rectificación, cancelación, oposición, portabilidad y limitación del tratamiento).
- Definir e Implantar las medidas técnicas necesarias para asegurar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales. Teniendo en cuenta en el contexto las técnicas de la naturaleza, el alcance y los riesgos
- Asumir el compromiso para minimizar las violaciones de seguridad, así como de colaborar con la autoridad de control Agente de Protección de Datos (ANTAI-AIG), para la resolución de incidentes o conflictos que puedan derivarse del incumplimiento de la normativa.
- Definir las responsabilidades necesarias y adecuadas para asegurar el cumplimiento de los requisitos de la normativa de protección de datos. Definiendo Políticas necesario aceptable que se consideren necesarias.

Esta Política proporcionará es el marco de referencia para el cumplimiento por parte de Syntegra Technology, de la normativa en materia de protección de datos, siendo comunicada a toda La Empresa y a las partes interesadas.

Para dar cumplimiento a esta Política de Protección de Datos Syntegra Technology ha procedido a la implantación de determinados procedimientos, medidas y normas de seguridad, así como a la definición de las Políticas necesarias para garantizar un nivel de seguridad adecuado de los tratamientos de los datos y la información.
En particular, los usuarios (colaboradores) deberán conocer y comprometerse a cumplir las siguientes normas:

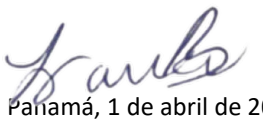
- Los activos de información (equipamiento informático, soportes, dispositivos móviles, aplicaciones…) pertenecen a La Empresa, el uso de estos debe emplearse exclusivamente con propósitos laborales, salvo autorización expresa por parte de la dirección. Es responsabilidad del usuario el cuidado y buen trato de los recursos informáticos y no informáticos asignados.
- Los equipos informáticos disponen de una configuración de seguridad por defecto. Los usuarios no deben modificar esta configuración, ni instalar o descargar, sin previa autorización, programas o software adicional, quedando expresamente prohibido el uso de software sin la debida licencia, que pueda suponer incumplimientos de la Ley de Propiedad Intelectual.

- No se podrán introducir en los sistemas o la red material o contenidos ilegales, obscenos, inmorales u ofensivos, carentes de los objetivos de La Empresa, o que pudieran atentar contra la moral o las normas deontológicas, o que pueda infringir los derechos de tercero.
- El usuario deberá guardar secreto profesional y máxima confidencialidad en relación con los datos de carácter personal a los que tenga acceso en virtud de su trabajo, así como cualquier otra información de la que tenga conocimiento como consecuencia de las actividades que desarrolle en La Empresa. Esta obligación subsistirá incluso después de finalizar sus relaciones con el responsable del tratamiento.
- No se deben crear ficheros, listados o conjuntos de datos personales sin la autorización de los responsables definidos, ni podrán comunicarse fuera de La Empresa sin contar con la debida autorización.
- Los usuarios deberán velar, por el cumplimiento de los principios y derechos de la normativa de protección de datos. Asegurando el cumplimiento del derecho de información cuando se obtengan datos personales.
- Deberán evitarse en la medida de lo posible la exposición o posibilidad de acceso a usuarios no autorizados de la información y en particular de los datos de carácter personal, a través de medios informáticos.
- Como norma general, los usuarios dispondrán de acceso únicamente a la información que precisan para el desarrollo de sus funciones. Se deberá notificar como incidencia si se detecta que se dispone de acceso a más información o más utilidades de las necesarias.
- Para controlar el acceso a la información, cada usuario dispondrá de un nombre y contraseña individual con permiso de acceso específico.
- Los usuarios son responsables del uso y custodia de las claves o contraseñas de acceso que se le asignen. En ningún caso deberán de ser comunicadas a otros usuarios, ni se registrarán o escribirán en ningún formato para evitar accesos no autorizados a las mismas.
- Queda expresamente prohibido el uso por parte de cualquier usuario el acceso y el aprovechamiento de los permisos de otros usuarios. Para instalar o modificar aplicaciones en los equipos de La Empresa, suplantando la identidad de otro usuario.
- Del mismo modo, se prohíbe expresamente intentar aumentar el nivel de privilegios de un usuario en el sistema, acceder a recursos sin autorización, uso no autorizado de contraseñas, explotación deliberada de vulnerabilidades y así como intentar distorsionar, falsear los logs o registros del sistema.
- El usuario solo debe utilizar el correo electrónico corporativo para los fines relacionados con las funciones y tareas que le han sido asignadas. El usuario es responsable de todas las actividades realizadas en su cuenta de correo. El cual no debe ser utilizado por personas no autorizadas.
- Es un deber de los empleados de La Empresa utilizar el servicio de correo electrónico de manera adecuada y responsable, ajustándose a las buenas prácticas que se definan a tal efecto: envíos de correos masivos o de tamaño elevado que puedan saturar la red, descarga de ejecutables o ficheros adjuntos sin verificar, envío de datos confidenciales sin cifrar, uso de firma corporativa…
- El uso de soportes externos u otros dispositivos de almacenamiento (lápices, USB, discos duros,…) para almacenar o trasladar información confidencial requerirán la autorización expresa de los responsables o de la dirección.
- Como norma general el acceso a Internet se limitará a finalidades relacionadas directamente con la actividad de La Empresa y las tareas del lugar de trabajo del usuario. Los usuarios no podrán acceder para descargar imágenes, vídeos, contenidos ilegales o contrarios a la moral y buenas costumbres.
- La Empresa puede facilitar a los usuarios dispositivos móviles para el desarrollo de sus funciones. En el cual se minimizará la información como norma general y su uso se limitará a fines estrictamente profesionales.
- Respecto al uso de estos elementos BYOD, se asegurará al menos: la existencia de sistemas antivirus, la correcta actualización de sistemas operativos, evitar accesos físicos de usuarios no autorizados, utilizar inicios de sesión o cuentas de usuario únicas, o no almacenar información en los mismos durante más tiempo del necesario.

- La Empresa se reserva el derecho a revisar, sin previo aviso, los usos realizados sobre los sistemas de información (logs de acceso, mensajes de correo electrónico, acceso a internet,…) con la finalidad de comprobar prevenir o reaccionar ante vulnerabilidades o incidentes de seguridad, y asegurar la integridad de los sistemas de información.
- El usuario debe custodiar y velar por la protección del dispositivo móvil asignado. Con bloqueo automático, acceso mediante contraseñas o patrones, conexión a redes inalámbricas conocidas o seguras, autorización para la instalación de software adicional, cifrado del dispositivo,...
- Se debe asegurar el respaldo de la información tratada en La Empresa, para lo cual se han definido los procedimientos adecuados, realizándose copias sobre los directorios, ubicaciones y sistemas necesarios. Los usuarios deben asegurar que la información que generan se encuentra en dichos directorios, y que no se encuentra únicamente en sus propios equipos a nivel local.

Para conocer con mayor detalle o profundidad las normas definidas por la organización, el usuario debe acceder a la "**Guía de Seguridad del Usuario"** que se incluye como anexo al presente documento. Que debe ser puesto a disposición de todos los usuarios con acceso a datos, así como al resto de Políticas y Normas que se hayan definido y comunicado por parte de la organización. Para acceso a cualquier interesado de manera pública se coloca a la disposición el correo electrónico contact@syntegracert.com.
El sistema de seguridad de la información y protección de datos abarca todas las actividades referentes a la Comercialización y servicios profesionales de software de gestión de base de datos en línea.

Alta Dirección



Panamá, 1 de abril de 2026.