POLÍTICA DE INNOVACIÓN Y VIGILANCIA TECNOLÓGICA

Sevilla, a 8 de enero de 2024.

El Consejo de Administración de TRACK GLOBAL SOLUTIONS,S.L. tiene atribuida la competencia de diseñar, evaluar, revisar aprobar y actualizar las políticas corporativas, las cuales contienen las pautas que rigen la actuación de la Sociedad.

En el ejercicio de estas responsabilidades, consciente de su compromiso con la importancia de la seguridad informática y la protección de datos, el Consejo de Administración aprueba esta Política de Seguridad Informática y Protección de Datos (la "Política"). La presente política establece las directrices para la protección adecuada de la información de la empresa y de sus clientes durante la ejecución de contratos de servicios de consultoría y formación, mediante el uso seguro de medios electrónicos. Esta política se aplica a todos los empleados, contratistas y terceros asociados con la empresa.

La presente política es aplicable a todo el personal que desempeña sus funciones en este centro de trabajo y a todos los trabajos que en él se desarrollen. Su vigilancia, operación y evaluación, estará a cargo de D. Kevin Guzmán Byrne.

1. Datos de identificación del centro de trabajo

Track Global Solutions,s.l.
Avenida Américo Vespucio 5-3. Planta 1.
41092 Sevilla (España)

2. Alcance

Esta política se aplica a todos los sistemas de información, dispositivos electrónicos, redes y medios digitales utilizados en la prestación de servicios de consultoría y formación, incluyendo, pero no limitándose a, ordenadores, teléfonos móviles, tabletas, servidores, aplicaciones en la nube, correos electrónicos y otros dispositivos de almacenamiento de datos.

3. Definiciones

- Información Confidencial: Datos de carácter sensible o valioso para la empresa o sus clientes, que requieren protección contra acceso no autorizado.
- Medios Electrónicos: Dispositivos y sistemas utilizados para el procesamiento, almacenamiento y transmisión de información digital.
- Usuarios Autorizados: Empleados, contratistas y terceros con acceso legítimo a los sistemas y datos de la empresa.

4. Principios de Seguridad

4.1. Control de Acceso

- **Autenticación:** Todos los usuarios deben autenticarse utilizando credenciales seguras antes de acceder a los sistemas de información.

- **Autorización:** El acceso a la información debe estar restringido según el principio de privilegio mínimo, otorgando solo los permisos necesarios para las tareas específicas relacionadas con los contratos de consultoría.

4.2. Protección de Datos

- **Encriptación:** La información confidencial debe cifrarse durante la transmisión y el almacenamiento utilizando algoritmos de encriptación robustos.

- **Clasificación de Datos:** La información debe ser clasificada de acuerdo con su sensibilidad, aplicando medidas de protección adecuadas a cada categoría.

4.3. Uso Adecuado de Recursos Electrónicos

- **Dispositivos Personales:** El uso de dispositivos personales para acceder o manejar información de la empresa debe estar autorizado y cumplir con las mismas normas de seguridad que los dispositivos corporativos.
- **Software y Aplicaciones:** Solo se debe utilizar software y aplicaciones aprobados por la empresa en dispositivos utilizados para fines de consultoría.

4.4. Monitoreo y Auditoría

- **Registro de Actividades:** Todas las actividades relevantes en los sistemas deben ser registradas y monitoreadas para identificar y responder a posibles incidentes de seguridad.
- **Auditorías Periódicas:** Se realizarán auditorías periódicas para verificar el cumplimiento de esta política y la eficacia de las medidas de seguridad implementadas.

5. Responsabilidades

Los Empleados y Usuarios Autorizados deberán cumplir con todas las directrices y procedimientos establecidos en esta política así como deberán reportar de inmediato cualquier incidente de seguridad o sospecha de violación.

La dirección de la empresa deberá asegurar que los empleados a su cargo comprendan y cumplan con esta política así como facilitar los recursos y la formación necesarios para el cumplimiento de las normas de seguridad.

6. Uso de Correo Electrónico y Comunicación Electrónica

- **Correos Empresariales:** Los correos electrónicos deben utilizarse para la comunicación oficial y deben ser enviados a través de cuentas de correo corporativas.

- **Mensajería Instantánea:** La información confidencial no debe compartirse a través de aplicaciones de mensajería instantánea no aprobadas.

- **Videoconferencias:** Las videoconferencias que involucren datos sensibles deben realizarse utilizando plataformas seguras y aprobadas por la empresa.

7. Manejo de Información de Clientes

- **Confidencialidad:** Toda la información relacionada con los contratos de consultoría y formación debe manejarse con estricta confidencialidad.
- **Almacenamiento Seguro:** La información de clientes debe almacenarse de forma segura y accesible solo para el personal autorizado.
- **Compartición de Datos:** La información de clientes no debe ser compartida con terceros sin el consentimiento expreso del cliente.
- **Medios de Transferencia:** La transferencia de información debe realizarse a través de canales seguros y cifrados.

8. Cumplimiento y Sanciones

El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la terminación del empleo, la suspensión del acceso a sistemas y datos, y la acción legal. La empresa se reserva el derecho de modificar esta política según sea necesario para cumplir con las normativas vigentes y adaptarse a nuevas amenazas de seguridad.

6. Vigencia

El presente Programa de Sostenibilidad Ambiental entrará en vigor en la fecha de su firma y será revisado cada cinco años.

David Parejo Sánchez
Consejero Delegado