INFORMATION SECURITY POLICY

1. OBJETIVE

The objective of this document is to serve as a guide for the Security and Privacy Information System Management, which pertains to the services provided by INNOIT and their associated infrastructure, as well as the protection of Personally Identifiable Information (PII).

The Information Security Management System (ISMS), in accordance with the current Statement of Applicability (SoA), covers the information systems that support the management of staffing services for the IT sector.
These services are delivered from INNOIT's facilities and from the facilities of the outsourced data processing center.

The scope of an information security policy should include all interested parties, meaning it should apply to all employees, suppliers, customers, and any other entity that interacts with the organization.

2. GENERAL INFORMATION

2.1. COMPANY PRESENTATION

INNOIT is a consulting firm specialized in technology and based in Barcelona, Spain. Founded in 2016, the company has established itself in the technology consulting market, offering innovative solutions to its clients to improve their performance and efficiency.

INNOIT's organizational culture is based on values such as innovation, integrity, and passion. The company fosters a positive work environment and a culture of continuous learning for its employees, offering the opportunity for professional development.

INNOIT works with a wide variety of clients from different industries. The company prides itself on offering customized solutions to each of its clients, ensuring that their needs are effectively and efficiently met.

In summary, INNOIT is a company focused on innovation and excellence, working to offer high-quality technological solutions to its clients and at the same time a positive work environment and continuous learning culture to its employees.

3.1. SECURITY POLICIES AND OBJECTIVES

INNOIT CONSULTING S.L., also known as INNOIT, acknowledges the crucial role of effective information security management in achieving business success and ensuring customer satisfaction. As a result, the company has adopted an Information Security Management System in accordance with the ISO-27001 standard.

To safeguard the confidentiality, integrity, and availability of all information, including personal data, INNOIT is committed to prevent against loss, disclosure, modification, or unauthorized use. To achieve this objective, the company is dedicated to developing, implementing, maintaining, and continuously improving its management system.

As a result, INNOIT offers its clients a secure environment where only authorized individuals have access to information that is maintained intact and available without manipulation. This information security policy applies to all system functionalities that we offer to our clients.

3.1 Security Objetives

The management is responsible for determining the objectives, analysing them, and using this analysis to define the organization's guidelines. To establish clear and achievable objectives, management evaluates various factors and works collaboratively with its team.

The security objectives established by the management are as follows:

1. **Protect the confidentiality of information**: The management establishes that its objective is to ensure the confidentiality of information handled in INNOIT, whether it is customer information, employee information, financial information, or information about ongoing projects.

2. **Ensure information integrity:** It is important that the information handled by the company is not altered. INNOIT establishes the objective of ensuring that the information remains intact and any unauthorized alteration is detected and corrected quickly.

3. **Ensure information availability:** Information is a critical resource for the company and INNOIT sets the goal of ensuring that information is available at all times, whether for employees, customers, or suppliers.

4. **Comply with standards and regulations**: INNOIT ensures compliance with ISO standards and regulations related to information privacy and personal data protection in its sector.

5. **Promote security awareness**: Information security is a team effort and management sets the goal of promoting security awareness among employees, so they know how to protect information and report any security incidents.

6. **Comply with customer contractual agreements**: INNOIT ensures that it complies with all the terms and conditions agreed upon with its customers to avoid contractual breaches.

7. **Ensure business continuity:** Management sets the objective of ensuring that the company is prepared to face any event that may affect business continuity, including cyber-attacks, natural disasters, or system failures.

8. **Ensure the secure and compliant use of Artificial Intelligence within the organization:** The company aims to ensure that the use of Artificial Intelligence tools and systems within the organization is carried out in a controlled, secure, and compliant manner, in accordance with applicable legal, regulatory, and contractual requirements, while protecting the confidentiality, integrity, and availability of information.

3. LEGAL COMPLIANCE

Ensuring legal compliance is critical for the protection of the company's information and for customer trust. InnoIT will stay up-to-date on the legal and regulatory requirements applicable to information security in order to ensure compliance.

4. CONTINUOUS EVALUATION AND IMPROVEMENT

The periodic review of the Information Security Policy is essential to ensure that it remains up to date and relevant at all times.

The Information Security and Privacy Policy shall always be aligned with the applicable national, European, and international data protection and privacy regulations, as well as with the information security standards and best practices adopted by INNOIT.

This Information Security and Privacy Policy may, at the discretion of the Committee, be communicated to interested parties, particularly customers and suppliers, in order to involve them in the continual improvement of the management system.

POLITICA DE LA SEGURIDAD DE LA INFORMACION

1. OBJETIVO, ALCANCE Y CAMPO DE APLICACIÓN

El presente documento constituye el manual del Sistema de Gestión de la Seguridad y Privacidad de la Información, en la prestación de los servicios ofrecidos por INNOIT en las infraestructuras especificadas y los PII's identificados.

El Sistema, según la declaración de aplicabilidad (SoA) vigente actualmente, abarca los sistemas de la información que dan soporte a la gestión de los servicios de personal para el sector TI.

La prestación de estos servicios se realiza en las instalaciones de INNOIT y en las del centro de procesamiento de datos subcontratado.

El alcance de una política de seguridad debe incluir a todas las partes interesadas, lo que significa que debe aplicarse a todos los empleados, proveedores, clientes y cualquier otra entidad que interactúe con la organización.

2. GENERALIDADES

2.1. Presentación de la empresa

INNOIT es un grupo de empresas de consultoría de tecnología informática que tiene dos sedes en España, la principal en Barcelona, la segunda en Madrid. Fundada en 2016, la empresa se ha establecido en el mercado de la consultoría tecnológica, ofreciendo a sus clientes soluciones innovadoras para mejorar su rendimiento y eficiencia.

La cultura organizacional de INNOIT se basa en valores como la innovación, la integridad y la pasión. La empresa fomenta un ambiente de trabajo positivo y una cultura de aprendizaje continuo para sus empleados/as, ofreciendo la oportunidad de desarrollarse profesionalmente.

El portfolio de clientes varía entre diferentes industrias. La empresa se enorgullece de ofrecer soluciones personalizadas a cada uno de sus clientes, asegurándose de que sus necesidades sean atendidas de manera efectiva y eficiente.

En resumen, INNOIT es un grupo de empresas enfocada en la innovación y la excelencia, que trabaja para ofrecer a sus clientes soluciones tecnológicas de alta calidad y en el mismo tiempo un ambiente de trabajo positivo y de aprendizaje continuo para sus empleados/as.

2.2. Políticas de Seguridad, Objetivos y Responsabilidades

La Dirección de INNOIT reconoce plenamente la importancia de una buena gestión de la seguridad de la información para el éxito de su negocio y la satisfacción de sus clientes. Por lo tanto, ha implementado un Sistema de Gestión de Seguridad de la Información conforme a la norma ISO-27001.

INNOIT se compromete a proteger la confidencialidad, integridad y disponibilidad de toda la información, incluyendo los datos personales, para evitar su pérdida, divulgación, modificación o uso no autorizado. Para lograr este objetivo, la empresa se dedica a desarrollar, implementar, mantener y mejorar constantemente su Sistema de Gestión.

Como resultado, INNOIT ofrece a sus clientes un entorno seguro donde solo las personas autorizadas tienen acceso a la información, que se mantiene íntegra y disponible sin manipulaciones. Esta política de seguridad de la información se aplica a todas las funcionalidades del sistema que se ofrece a cada cliente.

2.2.1.Objetivos de seguridad

La dirección de la empresa es responsable de determinar los objetivos, analizarlos y utilizar este análisis para definir las orientaciones de la organización. Para establecer objetivos claros y alcanzables, la dirección evalúa varios factores y trabaja de manera colaborativa con su equipo.

Los **objetivos de seguridad** establecidos por la dirección son los siguientes:

1. **Proteger la confidencialidad de la información:** La dirección establece que su objetivo es garantizar la confidencialidad de la información que se maneja en INNOIT, ya sea la información de los clientes, empleados/as, la información financiera o la información sobre proyectos en curso.

2. **Asegurar la integridad de la información:** Es importante que la información que maneja la empresa no sea alterada sin autorización. La dirección establece que el objetivo es asegurar que la información se mantenga íntegra y que cualquier alteración no autorizada sea detectada y corregida rápidamente.

3. **Garantizar la disponibilidad de la información:** La información es un recurso crítico para la empresa y la dirección establece como objetivo garantizar que la información esté disponible en todo momento, ya sea para los empleados/as, clientes y/o proveedores.

4. **Cumplir con las leyes, regulaciones y el GDPR:** La dirección establece como objetivo asegurarse de que la empresa cumpla con todas las leyes y regulaciones que se aplican a su sector, incluyendo las relacionadas con la privacidad de la información y la protección de datos personales.

5. **Promover la conciencia de seguridad**: La seguridad de la información es un esfuerzo de equipo y la dirección establece como objetivo promover la concienciación de seguridad entre los empleados/as, para que sepan cómo proteger la información y reportar cualquier incidente de seguridad.

6. **Cumplir con los acuerdos contractuales de los clientes**: INNOIT debe garantizar de cumplir con todos los términos y condiciones acordados con sus clientes para evitar incumplimientos contractuales, que puedan tener consecuencias financieras y legales significativas.

7. **Asegurar la continuidad del negocio:** La dirección establece como objetivo lo de asegurar de que la empresa esté preparada para enfrentar cualquier evento que pueda afectar la continuidad del negocio, incluyendo ataques cibernéticos, desastres naturales, cambios climáticos, o fallos en los sistemas.

8. **Garantizar el uso seguro y conforme de la Inteligencia Artificial dentro de la organización:** la empresa quiere garantizar que el uso de herramientas y sistemas de Inteligencia Artificial en la organización se realiza de forma controlada, segura y conforme a los requisitos legales, regulatorios y contractuales aplicables, protegiendo la confidencialidad, integridad y disponibilidad de la información.

3. Cumplimiento legal

Garantizar el cumplimiento legal es crítico para la protección de la información de la empresa y la confianza del cliente. INNOIT se mantiene actualizada sobre los requisitos legales y regulatorios aplicables a la seguridad de la información para poder garantizar el cumplimiento.

4. Revisiones y mejora continua

La revisión periódica de la política de seguridad de la información es esencial para garantizar que la política se mantenga actualizada y relevante en todo momento.

La Política de Seguridad y Privacidad se adecuará en todo momento a las disposiciones vigentes en materia de privacidad de los datos de carácter personal tanto a nivel nacional, internacional y nivel europeo y a los estándares y mejores prácticas de Seguridad de la Información adoptadas por INNOIT.

La presente Política de seguridad y Privacidad de la información podrá, según disponga el Comité, ser comunicada a las partes interesadas, y en particular a clientes y proveedores, con el fin de involucrarlos en la mejora continua del sistema.