GreenPowerIT

D6.1 Specification for companies

This project has received funding from the European Union's Digital Europe programme under **Grant Agreement No. 101083637**

Deliverable number :	D6.1
Due Date :	30/06/2023
Nature[1] :	R
Dissemination Level[1] :	PU
Work Package :	WP6
Lead Beneficiary :	CITC
Contributing Beneficiaries :	ALL

DOCUMENT HISTORY

Version	Date	Author	Description
0.1	01.06.2023	CITC	Creation Deliverable template
0.2	20/06/2023	CITC	Updates and completions
0.3	25/06/2023	CITC	Critical review and proofreading
0.4	30/06/2023	CITC	Final edits for approval
1.0	07/07/2023	CITC	Final version

Table of Contents

Acronyms

Acronym	Description
EDIH	European Digital Innovation Hub
HTTP	Hypertext Transfer Protocol is the underlying protocol used for transmitting and receiving data over the internet, allowing web browsers to communicate with web servers to access websites and retrieve information.
HTTPS	Hypertext Transfer Protocol Secure, and it's a secure version of HTTP that encrypts data sent between a web browser and a website, ensuring privacy and security during online communication.
SSH	Secure Shell is a secure network protocol that allows you to securely access and manage remote computers or servers over an unsecured network, like the internet.
AV	An antivirus is a software program that helps protect your computer or device from malicious software, such as viruses, by scanning files and detecting and removing any potential threats.
OAuth	OAuth is an authentication framework that enables users to grant limited access to their online resources to third-party applications or websites without sharing their passwords.
JWT	JSON Web Token is a compact and secure way to transmit information between parties, often used for authentication and authorisation in web applications.
SQL	Structured Query Language is a descriptive language used for managing and manipulating databases.
WAF	Web Application Firewall is a security measure that protects web applications from various online threats, such as malicious attacks, by monitoring and filtering the traffic between the application and the internet.

1. Introduction

1.1 Purpose and Scope of this document

The purpose of this document is to define the needs and requirements of the «XYZ» project precisely and comprehensively. Its aim is to establish a structured framework, enabling a common understanding among all involved parties. By clearly defining the objectives to be achieved, risks to be anticipated, as well as technical and environmental constraints, this document will serve as a reference throughout the project, ensuring its success.

1.2 References

1. Specifications for IT software development (accessed 15 June 2023): https://cahiersdescharges.com/telechargement/cahier-charges-developpement-logiciel-informatique/

2. Generic Model Annex CCTP (accessed 25 June 2023): https://ies-sud.fr/wp-content/uploads/2019/03/ICR-SI-SSI-LIV-1-Mode%CC%80le-ge%CC%81ne%CC%81rique-annexe-se%CC%81curite%CC%81-CCTP.pdf

3. Environmental clauses in building works or how to act differently (accessed 25 June 2023): https://www.achatpublic.info/sites/default/files/document/documents/les_clauses_environnementales_dans_les_operations_de_travaux_cg_somme_decembre_2014.pdf.

2. Stakeholders' Presentation

2.1 Service Provider Presentation

In this section, we will provide a detailed presentation of the service provider, who is the entity responsible for executing the "XYZ" project. We will highlight their expertise, experience, and specific skills that enable them to effectively undertake such projects. This presentation will provide the client with a clear understanding of the capabilities and references of the service provider.

2.2 Client Presentation

In this section, we will address the presentation of the client, the entity that will benefit from the "XYZ" project. We will provide relevant information about the client, such as their industry, strategic objectives, and specific expectations regarding the project. This presentation will enable the service provider to better understand the client's needs and requirements, and to tailor their approach accordingly.

3. Project Overview

3.1 Project Presentation

In this section, we will provide a comprehensive presentation of the "XYZ" project. We will describe in detail its context, scope, and key components. This presentation will establish an overview of the project, highlighting its specificities and unique aspects.

3.2 Project Objectives

In this section, we will specify the key objectives of the "XYZ" project. We will clearly define measurable targets that the project aims to achieve, in terms of expected outcomes, performance, functionalities, or other relevant criteria. These objectives will serve as a reference throughout the project to assess its success and alignment with expectations.

3.3 Project Cyber Security Risks

This section will be dedicated to the identification and analysis of cybersecurity risks within the scope of the "XYZ" project. We will examine potential threats, vulnerabilities, and security measures to be implemented to prevent and mitigate these risks. The objective is to ensure an adequate level of security and protect the assets and data involved in the project.

3.4 Environmental aspects of the project

In this section, we will address the environmental aspects of the "XYZ" project. We will identify potential impacts on the environment, such as energy consumption, waste management, greenhouse gas emissions, etc. We will also explore measures and practices aimed at minimizing these impacts, while ensuring compliance with applicable environmental regulations.

4. Needs and requirements

4.1 Functional requirements

In this section, we will provide a detailed definition of the functional requirements of the "XYZ" project. We will identify the key functions and required features, focusing on the critical actions and processes of the system. This thorough analysis of the functional needs will guide the design and development of the project, ensuring that it meets the specific expectations.

4.2 Security clauses for computer systems

In the present document, the licensee represents the provider of the project, and the ESTABLISHMENT represents the partner of the said project. The references R and M correspond to the "Recommend" and "Mandatory" clauses respectively.

The security of IT systems is of paramount importance for any project involving cybersecurity, artificial intelligence (AI) and the Internet of Things (IoT). Security rules and clauses play an essential role in defining specific requirements and ensuring that adequate measures are in place to protect sensitive information and prevent cyber-attacks.

This section deals with security clauses for IT systems, providing precise guidelines for guaranteeing an appropriate level of security. The clauses cover various aspects such as software, authentication, system protection, cryptography, maintenance, remote maintenance, Wi-Fi specifications, mobile means and confidentiality of hosted data.

By adopting these clauses, the project commits to implementing robust security measures in line with recognized standards and best practices. This ensures a reliable and secure environment, reducing the risk of data compromise and service interruption.

Close collaboration with security experts and technical teams is essential for effective implementation of security clauses. The suppliers and service providers involved must also be made aware of the importance of complying with these clauses, to guarantee the overall protection of the IT system.

By scrupulously respecting these security rules and clauses, the project will reinforce its security posture and protect itself against potential threats. IT system security is a major issue for data protection, confidentiality and user confidence.

Be sure to customise this list to your specific needs and adapt it to your project.

4.2.1 General software requirements

		Support	Evaluation
M	The holder undertakes to acquire and grant to the ESTABLISHMENT all user licenses necessary for the proper operation of the connected device, unless specific conditions apply. This applies to all software and logic layers used (OS, software packages, DB, remote maintenance, etc.).		
M	The licensee undertakes to install and activate only the software required for the device to function properly.		
M	The licensee undertakes to install and activate only the software required for the device to function properly.		
M	For open-source software, software conformity is the sole responsibility of the licensee.		
M	For freeware, software compliance is the sole responsibility of the licensee: they must also comply with security requirements.		
M	For SaaS (Software as a Service) software, software compliance is the sole responsibility of the licensee.		
M	The contractor's personnel must comply with the ETABLISSEMENT's Information System access and use charter during any installation or maintenance work. The contractor undertakes to inform its personnel of this.		
R	No version of the operating system should be installed that is not maintained by the publisher in terms of security updates, except in special cases requiring additional protection to be described.		

4.2.2 Authentication

		Support	Evaluation
M	Passwords for accounts required to administer the solution must be modifiable by the ESTABLISHMENT.		
R	In the case of N-Tier architecture, the origin of the connection will be part of the authentication process. Thus, when the application allows user identities to be propagated to the data, the user cannot connect directly to the DBMS. The access chain must therefore be guaranteed for each application layer.		

4.2.3 System protection

		Support	Evaluation
R	The licensee undertakes to implement the necessary measures and settings to protect its systems against viral and intrusive attacks. Should the need arise, it may deploy its own utilities and update policies; nevertheless, it would be appreciated if it would agree to integrate its systems into the ETABLISSEMENT's security approach, by installing the ETABLISSEMENT's antivirus software and integrating its systems into the security patch management rules in force for the rest of the IS. In the event of intrusion or contamination, the licensee is responsible for the vulnerability of its systems regarding public patches and virus definitions.		

4.2.4 Cryptography

		Support	Evaluation
M	In the case of web applications published on the Internet, the use of SSL is imperative. The contractor may use certificates supplied by the ETABLISSEMENT.		
M	The use of cryptography by applications must comply with market standards and the Référentiel Général de Sécurité (RGS).		
M	Data used for authentication must be encrypted during communication and storage.		

4.2.5 Maintenance

		Support	Evaluation
M	It is the responsibility of the licensee to ensure the security of its remote intervention platform (data and software).		
M	The ESTABLISHMENT reserves the right to carry out (or have carried out) periodic or ad hoc security checks on the holder's premises in order to ensure that the required level of security complies with the following requirements		
M	No remote-control tools may be installed on standard ETABLISSEMENT workstations as part of an application. The only remote-control tool authorized is the one used for system administration managed by the ETABLISSEMENT's IT department.		
M	The ESTABLISHMENT's personal or technical data (equipment configuration) used by the licensee's support teams must not be divulged (appropriate protection must be provided).		
M	It is the responsibility of the licensee to restrict physical and logical access to its workstations to authorized persons only (by raising awareness and providing appropriate security measures).		
R	The intervention is governed by a regulation, a contract or an agreement between the ESTABLISHMENT and the licensee, defining the commitments of each party, the practical terms and conditions, etc.		

4.2.6 Remote maintenance

		Support	Evaluation
M	The remote maintenance connection must be made via the secure Internet gateway provided by the ETABLISSEMENT (VPN IPSEC or VPN SSL). The request for this VPN must follow the ETABLISSEMENT procedure.		
M	No remote-control tools may be installed on standard ETABLISSEMENT workstations as part of an application. The only remote-control tool authorized is the one used for system administration managed by the ETABLISSEMENT's IT department.		
M	The licensee must have an anti-virus and security patch update policy applied to remote maintenance workstations.		
M	The licensee is committed to the security of the service, and its legal representative must sign the contractor's maintenance commitment supplied by the ISD, reminding him of the confidentiality of the data and committing him to informing his staff that all accesses and actions will be traced.		
M	It is the responsibility of the licensee to know in all circumstances the identity of any person who connects or has connected to the remote maintenance platform and to ensure traceability (this traceability may be communicated on request by the ESTABLISHMENT).		
R	The licensee can provide full details of maintenance procedures (HR requirements, repair times, etc.).		
R	Remote maintenance stations should be physically isolated from the licensee's local network.		

4.2.7 Wi-Fi specification (802.11G or 802.11B)

		Support	Evaluation
M	The encryption and integrity of information circulating on the network must be ensured by installing the WPA2 mechanism (version of the IEEE 802.11i standard certified by the Wifi Alliance) on the equipment concerned.		

4.2.8 Mobile equipment

		Support	Evaluation
M	All mobile devices must be encrypted (in compliance with the General Data Protection Regulation: GDPR) and the encryption keys must be provided to the ETABLISSEMENT.		

4.2.9 Guaranteeing the confidentiality of hosted data

		Support	Evaluation
M	The licensee undertakes to guarantee access to data to authorized persons only, in accordance with the needs of the ESTABLISHMENT.		
M	The licensee undertakes to destroy the data at the end of the contract after returning it to the ETABLISSEMENT in a usable form.		
R	Contributors will be identified and asked to sign an individual confidentiality agreement. Access and actions carried out can be traced.		

4.3 Environmental clauses

Environmental clauses are of the utmost importance in all digital projects. These clauses are essential to promote sustainable development and ensure compliance with current environmental laws and regulations.

Among these laws, French law AGEC plays a critical role. It emphasizes the responsible management of electronic waste and the promotion of equipment reparability. By including this law in the environmental clauses, the project commits to respecting these legal provisions to reduce environmental impact and promote more sustainable practices.

In addition, the French REEN law requires an analysis of the project's lifecycle to identify the critical stages in terms of energy consumption, carbon emissions and environmental impact. The equivalent of this law could be the European ErP law (Energy-related Products). This analysis will enable appropriate improvement measures to be put in place, promoting a more environmentally friendly approach.

Environmental clauses also encourage the use of energy-efficient technologies, software and infrastructure, and the optimisation of energy consumption throughout the project life cycle. This helps to reduce carbon footprints and promote responsible use of energy resources.

The sustainability of products and components is also considered. The clauses encourage the use of sustainable, resource-efficient and recyclable solutions, wherever possible, to minimize environmental impact.

By incorporating these environmental clauses, the project is part of a responsible approach and actively contributes to sustainable development. It promotes compliance with environmental laws and regulations while encouraging environmentally friendly practices, thus creating a long-term positive impact on our planet.

		Support	Evaluation
M	Management of electronic waste: The licensee shall implement measures for the responsible management of electronic waste generated during the project, in accordance with applicable regulations.		
M	The licensee shall make every effort to achieve a design that facilitates the dismantling and repair of project equipment.		
M	Compliance with the AGEC law: The contractor undertakes to comply with the provisions of the AGEC law, regarding the management of electronic waste, the promotion of the reparability of devices, the encouragement of the circular economy and the limitation of programmed obsolescence.		
M	Lifecycle analysis: The licensee will carry out a lifecycle analysis of the project, in accordance with the REEN law, to identify the critical stages in terms of energy consumption, carbon emissions and environmental impact, and will propose appropriate improvement measures.		
M	Energy performance: The licensee undertakes to use technologies and equipment with optimum energy performance, in accordance with the REEN law, promoting energy efficiency and reducing carbon emissions.		
R	Energy consumption: The licensee will promote the use of energy-efficient technologies, software and infrastructure, as well as the optimization of energy consumption throughout the project life cycle.		
R	Durability of products and components: The licensee will promote the use of sustainable, resource-efficient and recyclable products and components wherever possible.		
R	Awareness-raising and training: The licensee will encourage awareness of environmental issues among project stakeholders (in-house staff, suppliers, end-users) and promote ongoing training in sustainable development.		

4.4 Technical requirements

This section will outline the technical requirements of the "XYZ" project. We will specify in detail the technical criteria that need to be met, such as performance, development standards, required technologies, client's financial and technical constraints, etc. The technical requirements will be addressed based on the following categories:

4.4.1 Client Requirements

We will provide a detailed description of the client's specific requirements in terms of technical, financial, and legal constraints. This may include specifications, cost limitations, existing infrastructure constraints, compatibility with other systems, etc. The objective is to meet the client's expectations while adhering to their constraints.

4.4.2 Cybersecurity Requirements

We will review the cybersecurity requirements for the "XYZ" project. This will include data protection, security measures, access controls, security audits, etc. We will ensure that the developed system or solution adheres to security standards and best practices in cybersecurity.

Please customise the list below to your specific needs and adapt them to your project.

NEEDS AND REQUIREMENTS

SOFTWARE:

Network:

	Support	Estimate
Secure configuration of firewalls to control traffic entering and leaving the system.		
Use of secure communication protocols (such as HTTPS, SSH, etc.) to encrypt data during transfer.		
Monitoring and detection of intrusion attempts and suspicious activity to quickly detect and respond to attacks.		
Use of a malware detection system (AV) to identify and eliminate potential threats.		

Web service:

	Support	Estimate
Use of robust authentication mechanisms (such as OAuth, JWT, multi-factor identification, etc.) to verify the identity of users and services.		
Rigorous validation and filtering of user input to prevent injection attacks (such as SQL attacks) and data manipulation vulnerabilities.		
Use of a Web Application Firewall (WAF) to filter and block attacks targeting web applications.		
Secure management of user sessions and access tokens to prevent unauthorized access.		
Browser security using strict security policies (such as Content Security Policy, HTTP Strict Transport Security, etc.).		
Secure data exchanges with customers using encryption, digital signatures, etc.		

NEEDS AND REQUIREMENTS

System:

	Support	Estimate
Use of regular operating system and third-party software updates to correct known vulnerabilities.		
Secure configuration of file and directory access rights to limit excessive authorisations.		
Use of encryption mechanisms to protect stored sensitive data.		
Application of password management (complexity, regular rotation, etc.) to reinforce authentication.		
Logging and monitoring of system events to detect abnormal behavior and attack attempts.		
Regular assessment of software security through penetration tests and audits to identify and correct vulnerabilities.		

NEEDS AND REQUIREMENTS

HARDWARE:

Components:

	Support	Estimate
Use of chips without pin access to limit the possibility of intercepting or manipulating signals.		
Use of secure chips with encoding mechanisms to prevent unauthorized duplication and manipulation of components.		
Concealment of component names and use of obfuscation techniques to make reverse engineering and understanding of hardware design more difficult.		
Use of anti-evasion enclosures and black-coated components to conceal hardware and reduce the risk of manipulation or physical compromise.		
Use of hardware security modules, such as Secure Elements or integrated hardware security modules to protect keys and sensitive data.		
Implementation of physical intrusion detection mechanisms, such as vibration sensors or casing sensors, to detect any attempt to open or compromise the hardware.		
Regular assessment of hardware security through penetration tests and audits to identify potential vulnerabilities and quickly correct them.		

Motherboard:

	Support	Estimate
Removal of debug connectors and programming interfaces to restrict unauthorized access to hardware components.		
Use of multi-layer designs to reinforce the physical strength and security of hardware components.		
Removal of test points to reduce risks of compromise and exploitation.		
Use of blind vias to reduce the risk of physical manipulation of internal connections.		
Use of physical protection mechanisms, such as tamper-proofing, to detect attempts at physical manipulation or intrusion on hardware components.		

Firmware:

	Support	Estimate
Deactivation of logging to prevent leakage of sensitive information.		
Secure updates using integrity verification and authentication mechanisms to guarantee the integrity and origin of firmware updates.		

4.4.3 Environmental Requirements

We will consider the specific environmental requirements of the project. This may include compliance with environmental regulations, reducing environmental impact, using sustainable resources, etc. We will also ensure that the project complies with legal requirements related to the environment.

Please customise the list (below) to your specific needs and adapt them to your project.

	Support	Estimate
Energy efficiency: Design devices, algorithms and systems optimized to minimize energy consumption.		
Sustainable resources: Use sustainable and recyclable materials and components.		
Carbon reduction: Minimize the carbon footprint throughout the project lifecycle.		
Efficient data management: Optimize data management to reduce energy consumption and storage capacity.		
Recycling and e-waste management: Promote responsible recycling of end-of-life devices.		
Renewable energy sources: Integrate renewable energy supply solutions.		
Environmental regulatory compliance: Respect local regulations concerning waste management and the use of hazardous substances.		
Energy efficiency monitoring: Track energy consumption to optimize performance.		