OSF | DIGITAL

Calea Plevnei nr. 159, Cladirea C,
Etajul 4, Sector 6, Bucuresti, Romania
Fax: +40 (31) 710 72 91
osf.digital

Technical and organizational security measures

This Annex describes technical and organizational security measures implemented by OSF to protect personal data and ensure the ongoing confidentiality, integrity and availability of OSF products and services in accordance with article 32 of EU general data protection regulation 2016/679.

This document is an overview of OSF technical and organizational security measures. More details on the measures implemented are available upon request sent to dataprotection@osf.digital, or otherwise made reasonably available by OSF. OSF reserves the right to revise these technical and organizational measures at any time, so long as any such revisions will not materially reduce or weaken the protection provided for personal data that OSF processes in providing its various services.

OSF implements the following technical and organizational security measures to protect personal data:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of OSF information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the OSF, monitoring and maintaining compliance with OSF policies and procedures, and reporting the condition of its internal management.

3. Maintain Information security policies and make sure that policies and measures are regularly reviewed and, where necessary, improve them.

4. Data security controls which include logical segregation of data, restricted (e.g. role-based) access and monitoring, and where applicable, utilization of commercially available and industry-standard encryption technologies.

5. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

6. Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.

7. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

8. Physical and environmental security of data center, server room facilities and other areas containing client confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of OSF facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

9. Change management procedures and tracking mechanisms to designed to test, approve and monitor all changes to OSF technology and information assets.

10. Incident / problem management procedures design to allow OSF investigate, respond to, mitigate, and notify of events related to OSF technology and information assets.

11. Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

12. Business continuity and disaster recovery procedure, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

13. Training - Personnel training in data protection and security procedures (e.g. use of passwords and access to specific data processing systems). Information on specific data protection legal obligations is also central, especially for key personnel involved in high-risk processing of personal data.

14. Back-ups - A back-up system is an essential means of recovering from the loss or destruction of data. While some systems should be in place, the frequency and nature of back up will depend, amongst other factors, on the type of organization and the nature of data being processed. Under GDPR Article 32 the aspect of the "ability to restore the availability and access to personal data" in part of the data security obligations for the data controller or data processor.

15. Data deletion/disposal - The purpose of disposal/deletion is to irreversibly delete or destroy personal data so that it cannot be recovered. The methods used must, therefore, match with the type of storage technology, including paper-based copies.

16. Security and confidentiality of personal data - Based on a risk assessment, OSF ensures a level of security appropriate to the risk, including inter alia as appropriate:

- the anonymization, pseudonymization and encryption of Personal Data.
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
- ensure a logical separation between its own data, and the data of its customers and suppliers.
- setup a process to keep processed data accurate, reliable and up to date.

17. Organization control - OSF maintains its internal organization in a manner that meets the requirements of the applicable data protection legislation, and this shall be accomplished by internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations, as follows:

a) Protection of global personal data policy:

The policy refers to all parties (employees, job candidates, customers, suppliers, etc.) who provide any amount of information to OSF. This Global Personal Data Protection Data Policy is the foundation of that data protection and privacy program and describes the approach taken by OSF when processing Personal Data anywhere in the world. The Procedure applies globally to OSF processing of Personal Data, whether by electronic or manual means (i.e., in hard copy, paper, or analog form). All OSF entities and employees shall comply with this Global Personal Data Protection Data Policy.

b) Personal Data Protection Policy in the development process:

The policy applies to all OSF employees and furthermore to all roles involved in project development. Designers, developers, publishers, solution architects, project managers, team leaders, owners need to fully understand the Core Data Protection Principles, Rights of individuals and how to handle/implement those within the SDLC and Personal Data Processing Lifecycle, through the chapters of this document.

c) Data Classification Policy

The scope of the policy is to establish a structured and consistent classification framework for defining the company's data security levels. The purpose of the policy is to protect the privacy of OSF customers, partners, and staff, as well as to protect the confidentiality of important information within the organization. The policy applies to all OSF employees, customers, vendors, contractors, trainees, and volunteers, and it is applicable to all Data as defined in the policy. However, it does not apply to personal property of individuals covered by the policy, such as personal notes unrelated to company operations.

d) OSF Security Policy:

The policy covers the following: confidentiality of data, Access to OSF resources and data, licensed software requirements, data transfer principles, removable media management, password management, antivirus, firewall, physical security, resources availability, business continuity, documents and data sharing, assets management.

e) Security Policy for Physical Access

The focus is to ensure that access to server rooms and IT equipment rooms is restricted to authorized personnel only. This is achieved through various measures such as securing the doors, implementing authentication methods, and monitoring the rooms. The policy also emphasizes the need for a complete inventory of equipment and the restriction of physical access for former employees. Additionally, the policy outlines rules for building access, including the use of access cards or codes, escorting visitors, and reporting any unauthorized access.

f) Identity & Access Management Policy

OSF recognizes the importance of Identity and Access Management as a crucial cybersecurity capability. The company is committed to ensuring that individuals are granted appropriate access to resources based on their roles and responsibilities. To enhance the field of identity and access management, OSF conducts targeted research to gain insights into emerging technologies, their influence on existing standards, and the effective implementation of identity and access management solutions.

The purpose of this policy is to define and establish the needed requirements to protect the privacy, security, and confidentiality of OSF resources through access control measures.

g) Vulnerability and Patch Management Policy

The policy defines requirements for the management of information security vulnerabilities and the notification, testing and installation of security-related patches on devices connected to company networks. The policy applies to all OSF employees who have access to company's information, information systems or IT equipment as software, servers, desktops, laptops, mobile devices and IT appliances owned and operated by OSF.

h) Monitoring, measurements, analysis, and evaluation of OSF systems Procedure

The purpose of this procedure is to describe the periodical checks concerning the operational control, compliance, Sustainability & Human Resources and security areas, in order to ensure conformity with the quality, compliance, Sustainability & Human Resources risk and security standards requirements, in accordance with ISO 9001:2015, ISO 27001:2022 and GDPR in the current activity of OSF.

i) Data breach incident detection and response procedure:

The focus of any breach response plan should be on protecting individuals and their personal data, together with business' critical assets and data. Consequently, breach notification should be seen as a process for enhancing compliance in relation to the protection of personal data. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across OSF.

The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

j) Data Wiping Procedure:

The purpose of this procedure is to address the reliable erasure and destruction of business, personal and sensitive data that is stored electronically and non-electronically (e.g. paper, DVD). This procedure is in relation with the core 'data minimization' GDPR principle, outlined in the Protection of Personal Data Global Policy. Official company records (electronic or paper) must be appropriately retained based on the company's records retention policy, prior to erasure or destruction of the document, system, device or media.

k) Disk Encryption User Guide:

Full disk encryption is a technique, with high privacy benefits and relatively easy to use.
The solution provides strong encryption, and it comes built in to all major operating systems.
It is the only way to protect the data in case the laptop (computer) is lost or stolen, and it takes minimal effort to get started and use.

l) Password management tool – User Guide:

All OSF employees manage their password through an approved password management tool in order to secure and protect them properly.

m) PC usage guide. Best practices and Security Guide:

The document covers organizational instructions and rules for: computer naming instructions, Antivirus setup, software updates, password management, email instant messaging and web browsing policy, sign-in/out/lock from PC, restrict remote file access, back-up, data removal.

n) Secure Data Transfer Best Practices

This annex details secure methods for data transfer between internal employees and also between business partners and employees.

The overall purpose of this policy is to inform employees on best practice when securely transferring information. This is to reduce the risk of unauthorized disclosure of such information that could lead to a breach of confidentiality. The policy requires employees to consider the various methods available to transfer information and to ensure that security provisions are applied to every selection.

The policy also identifies the risks when transferring personal information and requires employees to consider these in line with legislation.

o) Business Continuity Plan

Business Continuity Plan (BCP) is the process involved in creating a system of prevention and recovery from potential threats within OSF. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.

BCP involves defining any and all risks that can affect the company's operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters—fire, flood, or weather-related events.

p) Remote work Policy

The Remote Work Policy is an agreement that describes everything needed to allow OSF employees to work from home without causing any disruption to company goals and procedures. The policy outline who can work from home, how they should go about working from home, what is expected of them, how their work will be measured, what support is available to them, and their legal rights as remote work employees. OSF is committed to support homeworking, to enable the company to maximize its employee’s effectiveness, productivity, and efficiency, at the same time giving more flexibility in their working lives. The company provides the environment and tools to reap the benefits of adopting flexible working practices that meet the security needs of the business, the team and the individual.

MODIFICATION/REVISION REGISTRATION FOR:

“Technical and organizational measures”,

DOCUMENT CODE: BCR-OSF-01_A7

	Performed modification				Modification operator		
#	**No. §**	**Page**	**Date**	**Modification generating document**	**Name**	**Sign.**	**Date**
1	**Ed.1/Rev.1**	**4-5/6,** 17	18-Mar-24	Added security related procedures and policies	Roxana Radulescu		18-Mar-24
2							
3							
4							
5							
6							
7							
8							
9							