DUCHENNE
DATA FOUNDATION

Security Policy

Information Systems Security and Data Privacy Policy (The Short Version)

Revision 1.0 | Apr 2020

Revision History

Revision	Date	Author	Notes
1.0	13 Apr 2020	Christos Koziaris	Final Draft Version

	Composer	Approved by
Position		
Name		
Signature		
Date		

Glossary

Data Controller	Data 'controller' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	Data 'processor' means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

1. **PURPOSE OF THIS DOCUMENT**

This document summarizes the main points of the Information Systems Security and Data Privacy Policy for the Duchenne Data Foundation (DDF).

1. **Basic Principles Of Security Policy**

The information systems Security Policy and all issues, control points, procedures and reports that include, governed by a set of key principles that should be complied by all roles involved in the use, management, and development of information systems of DDF. Such control points help to ensure the operation of the organization, namely DDF to:

- Ensure the confidentiality, integrity and availability of information,
- Give equal treatment to all users of DDF,
- Implement all the necessary measures to ensure the confidentiality and privacy of sensitive information collected from patients by DDF systems and users who process such data.

1. **Policy Summary**

This text summarizes the official DDF Information Systems Security and Data Privacy Policy (ISSDPP). The purpose of such a policy is to put the necessary security requirements and measures in order to ensure the confidentiality, integrity and availability of data and operational resources of DDF. Security rules and regulations described in this text are progressively applied through specific security measures.

This short version stands for information purposes, to all stakeholders.

The ISSDPP policy plays an important factor in the ability of DDF to work seamlessly and its application helps support of operational activities. In addition, the development and implementation of the policy contributes to compliance with the specific requirements of DDF independence, transparency and confidentiality arising from the regulatory and legal framework governing DDF operation.

The development and maintenance of this security policy aims:

- To serve as a point of reference for all matters directly or indirectly related to data security,
- To provide guidance in the selection and implementation of security measures and countermeasures,
- To strengthen the "channels of communication" between the stakeholders and the interested parties,
- To secure and manage resources,
- To consolidate the importance of security of Information Systems,
- To assist in growing a "security and privacy culture and philosophy" on the human factor,
- To ensure the confidentiality, integrity and availability of sensitive information and data in DDF systems, users and researchers that manage such information.

The ISSDP identifies the roles, responsibilities, and competencies of members of DDF directly related to its implementation.

1. **Governance and Policy Chapters**

DDF at regular intervals or in cases of significant changes reviews and revises the security policy, to ensure the following:

- Align with the organization needs and the organization's strategy.
- Ensure the adequacy of the protective measures foreseen in relation to the risks facing computer systems.
- Achieve compliance with regulatory requirements, especially as regards the protection of commercially or personal sensitive information and the equal treatment of users of DDF, and the privacy of the patient's data collected.

During the review, all elements that contribute to the formation of an integrated picture of the operational environment and information systems of DDF during

the current period are considered. Specific elements to be considered are the following:

- The current situation and the level of preventive and remedial security measures.
- The results of previous information security and privacy audits made by the administration or by independent bodies.
- The recommendations regarding the proper implementation of the compliance program of DDF Information Systems Security and Data Privacy Policy, to remain aligned with the regulatory requirements.
- Logging of changes made since the previous review of the policy (changes in business processes, legislative and supervisory framework, in technical equipment and staff).
- The (revised) analysis of possible existing or new risks.
- The evaluation of modern methods of attack in information systems for the integrated approach to security threats and vulnerabilities.
- Reports about incidents of a security or privacy breach of Information Systems.

DDF maintains and develops policies for

- The classification and management of data and information that processes.
- The acceptable use of its information systems by all stakeholders
- The access password principles and management
- Security Incidents management
- Periodic inspections to validate and strengthen security
- Information Systems Backup and Business Continuity Management
- Cloud Services providers assessments
- Periodic review of the security management system along with updated risk assessments