DUCHENNE
DATA FOUNDATION

# Information Security and Data Privacy Management System (Short Public Version)

**Revision 2.0 | Mar 2022**

# Table of Contents

# 1 Glossary

| Term | Definition |
|---|---|
| | |
| **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. |
| | |

# 2 Acronyms

| Acronym | Definition |
|---|---|
| | |
| **DDF** | Duchenne Data Foundation |
| **DM** | Duchenne Map |
| **ISDPMS** | Information Security and Data Privacy Management System |
| **IT & IS** | Information Technology & Information Systems |
| **ISMSC** | ISMS Committee |
| **ISO** | Information Security Officer |

# 3 Purpose of this Document

This document summarizes the main points of the Information Security and Data Privacy Management System (ISDPMS) for the Duchenne Data Foundation (DDF) data, information and its digital applications: Duchenne Map, BIND Duchenne Database and Duchenne Repository.

# 4 Basic Principles

The Information Security & Data Privacy Management System includes policies, control points, and relevant procedures and reports, which are 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 DDF to:

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

# 5 Policy Summary

This text summarizes the official DDF Information Security and Data Privacy Management System (ISDPMS). The purpose of such a system is to -define and enforce 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 public version was created for information purposes, to all DDF stakeholders (see chapter 6.17, Appendix B |Interested Parties, page 16).

The ISDPMS plays an important factor in the ability of DDF to work seamlessly and its application helps support of operational and data processing activities. In addition, the development and implementation of the system contributes to compliance with the specific requirements of DDF independence, transparency and confidentiality arising from the Regulatory and Legal framework governing DDF operation as described in the ISMS manual.

The development and maintenance of the ISDPMS 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, and potential users that manage such information.

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

# 6 Governance and Policy Chapters

DDF at regular intervals or in cases of significant changes reviews and revises the information security policies as described in the ISMS manual, so as 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 information 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 taken into account. Specific elements to be taken into account 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 ISDPMS, to remain aligned with the regulatory requirements;
- Logging of changes made since the previous review of the system (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 Information Security 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.

## 6.1. Policy statements

DDF Information Security Policy follows the principles, guidelines and responsibilities as set out in the Information Security Management System (ISMS) ISO/IEC 27001:2017. These include:

- Data is protected in line with relevant EU legislation, notably those relating to Data Protection, Human Rights and Freedom of Information as well as relevant DDF policies;
- Each information asset group has a nominated owner responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset;
- Data is made available solely to those who have a legitimate need for access;
- All data is classified according to an appropriate level of security;
- The integrity of data is maintained;
- It is the responsibility of all individuals who have been granted access to data to handle it appropriately in accordance with its classification,
- Data is protected against unauthorized access;
- Compliance with the Information Security Policies is enforced;
- DDF follows a risk-based approach to Information Systems Security. To determine the appropriate level of security control applied to IT systems, a risk assessment identifies the likelihood and impact of a security incident and define security requirements. The Information Security Officer (ISO) and the Data Protection Officer (DPO) can provide advice for an Information Security Risk Assessment;
- This policy follows ISO 27001 Information Security Principles and the fourteen sections below address one of the defined control categories.

## 6.2. Information security policies

**6.2.1.** Further policies, procedures, standards and guidelines exist to support the Information Security Policy and have been referenced within the text. Further information is available for staff in the DDF.

**6.2.2.** The current Information Technology (IT) & Information Systems (IS) security related DDF' Policies are listed in chapter 6.16 of ISDPMS, Appendix A |

## 6.3. Organization of information security

**6.3.1.** DDF has defined and implemented roles for the management of information security. This includes identification and allocation of security responsibilities to initiate and control the implementation of information security across DDF.

**6.3.2.** The hierarchy of responsibility is:

- ISMS Committee (ISMSC) is accountable for the DDF ISMS Risk Register;
- The ISMSC has representatives from all relevant sections of DDF and its purpose is to influence, oversee, promote and improve information security by identifying and assessing security requirements and risks;
- The Information Security Officer supported by the IT & IS Leadership Team,

Governance and Legal Services and the Data Protection Officer, manages information security, providing advice and guidance on the implementation of this policy;

- Information owners for IT systems, such as Business Service Owners are responsible for compliance with this policy;
- IT Admins/System Owners are responsible for ensuring that appropriate security arrangements are in place for IT administrative access and security controls on managed systems are compliant;
- Information users assume local accountability for data management and compliance with this policy. They are responsible for reporting any actual or suspected breach in information security or any working practice that increases the risk of a potential information security breach.

### 6.4. Human resources security

**6.4.1.** All approved users of DDF including IT services must demonstrate an understanding of the GDPR 2016/679 and the ISMS. Staff is trained and attends “Information security awareness” courses.

**6.4.2.** The policy and expectations for acceptable use are communicated to all users of DDF. Breaches of policy are handled by staff line management with assistance from the ISO.

**6.4.3.** Security responsibilities are included in job role descriptions, person specifications and personal development plans. Users accessing DDF data must seek advice from IT&IS and/or ISO if in any doubt of responsibilities.

**6.4.4.** Employee signed contracts enforce compliance with DDF policies.

**6.4.5.** Upon termination of a staff appointment, Human Resources will revise the staff record system, accordingly, triggering IT systems account termination processes. Not all system access is automatically controlled, for example local systems and records. Therefore, Line Managers must ensure that appropriate staff exit procedures are in place to remove access to all systems upon staff exit or change of role.

**6.4.6.** Line managers must ensure that all IT assets owned by DDF must be returned upon termination of contract.

**6.4.7.** The ISO may authorize legally compliant monitoring of IT systems to investigate security incidents and compliance with DDF policies.

## 6.5. Asset management

**6.5.1.** All assets (information, data, software, processing equipment and IT services) will be identified and owners documented to be responsible for the maintenance and protection of those assets in accordance with DDF's policies. All data created, received or retained must be protected according to the DDF data classification as defined in the ISMS (see chapter 6.18, Appendix C | ) and the relevant Classification Information Policy - Brief details are given below, and more detailed advice is available from Governance and Legal Services. The four DDF data classifications are:

- Confidential – The information assets which have high confidentiality value belong to this category. Only a limited set of authorized users shall access these information assets. Examples include business strategy, personnel files and patients' data.
- Project / Process / Department specific – The information assets that contain data pertaining to the needs of a specific department, project team, or business process, belong to this category. Such information assets shall be accessible to members of the concerned department, project, or business process only. Examples are financial data, project planning, contact lists, policies and procedures.
- Internal – The information assets which can be distributed within all offices of DDF belong to this category. Examples are office orders and internal circulars.
- Public – The information assets which do not have any confidentiality requirement and / or can be disseminated to the general public belong to this category. Examples include the annual financial report of DDF, public policies and information displayed on DDF's website.

**6.5.2.** All DDF information assets will follow the DDF Retention Schedule. Data must be stored on facilities provided by DDF as advised. Protected and Restricted data must not be stored on desktop computers or any unencrypted device. Email is a communications mechanism and must not be used as a replacement for file storage.

**6.5.3.** Mass storage devices such as CDROM, DVD, memory cards or USB drives should be treated in the same way as Protected/Restricted data and must be locked away at the end of the working day. For further guidance for staff refer to the IT&IS DDF page on file storage.

**6.5.4.** Dispose of physical records containing Protected/Restricted data securely by using provided confidential waste shredding services or shredders.

## 6.6. Access control

**6.6.1.** A procedure for user account creation and deletion is maintained for access to all IT systems. Access is granted according to an individual's role and the data classification.

**6.6.2.** Mandatory authentication is used wherever technically possible. Multi factor authentication is also for accessing Protected/Restricted data, where this service is provided by DDF. Users with administrative rights use their normal user accounts for standard IT system access and only use elevated privileges when required. Administrative account passwords conform with the Password Policy.

**6.6.3.** Users do not share their login details to access IT services. Passwords are in accordance with the Password Policy.

**6.6.4.** All IT equipment and systems connected to the DDF network or connecting remotely meet the minimum specification defined in the relevant policies (see PART D | Securing the Systems in chapter 6.16, Appendix A |ISMS related DDF's Policies, page 15), utilizing an operating system still receiving security updates with antivirus software installed.

## 6.7. Encryption

**6.7.1.** DDF IT&IS provides guidance and tools to ensure proper and effective use of encryption to protect the confidentiality and integrity of data and IT systems. Where IT&IS manages devices, the encryption keys will be securely managed.

**6.7.2.** Where a staff member manages their own encryption, it is critical that encryption keys are securely backed up, as forgetting an encryption key will mean the encrypted data is lost forever.

**6.7.3.** Data encryption is required for Protected/Restricted data transmitted over data networks. Protected/Restricted data is encrypted if stored away from the DDF.

## 6.8. Physical and environmental security

**6.8.1.** Data centers, computer rooms, and communications facilities used for hosting equipment for information processing, are physically protected from unauthorized access to prevent theft or damage. Facilities are adequately protected against environmental damage such as by fire or flood.

**6.8.2.** Computer equipment is password protected if left unattended. Screen locks are activated when there is no activity for a short period of time. Passwords must not be written down anywhere near IT equipment.

## 6.9. Operational security

**6.9.1.** Operational changes to equipment, infrastructure, or software affecting DDF's Production IT services and suppliers must follow IT&IS change management procedures.

**6.9.2.** IT&IS provide backup services for managed storage. Information/System owners must ensure that appropriate backup and system recovery measures are in place for locally managed and third-party services they use. Appropriate security measures must be taken to protect against damage or loss of backup media. Backup recovery procedures must be tested on a regular basis.

**6.9.3.** It is not permitted to connect personally owned equipment to any network socket; personally, owned devices use the wireless network.

**6.9.4.** Any device connected to the DDF network must comply with the Patching Policy. Devices which are not compliant will be liable to physical or logical disconnection from the network without notice. All devices connected to the network, irrespective of ownership, are subject to monitoring and security testing.

**6.9.5.** Individuals installing software themselves are responsible for that installation. Those responsible for software must monitor relevant sources of information for security update alerts.

**6.9.6.** DDF inspects systems connected to our network for vulnerabilities. If critical and high vulnerabilities are detected that cannot be mitigated, the system will be disconnected from the network.

**6.9.7.** DDF follows the ISMS policies for monitoring the Operating Systems Logs (see PART D | Securing the Systems and PART F | Cybersecurity and Incident Response in chapter 6.16 Appendix A |ISMS related DDF’s Policies, at page 15 )to monitor controls implemented within the Organization for logging and monitoring.

### 6.10. Communications security

**6.10.1.** DDF maintains network security controls to ensure the protection of data within its network and the internet.

**6.10.2.** Segregation exists between wired and wireless traffic and Production, Development, Test and management services according to data classification. Appropriate controls are enforced between security zones to reduce the risks of compromise, denial of service attacks, malware infection and unauthorized access to data.

### 6.11. System acquisition, development and maintenance

**6.11.1.** Information security requirements must be defined during the development of business requirements for new IT systems and reviewed following significant changes to existing IT systems. IT&IS provides advice on the security requirements for new IT services and significant changes to existing IT services.

**6.11.2.** All new projects that will implement systems that process personal data seek advice from the ISO and DPO during the development of business requirements.

### 6.12. Supplier relationships

**6.12.1.** Suppliers follow DDF security policies, change control process and support arrangements. Contact IT&IS Service Desk for further guidance.

### 6.13. Information security incident management

**6.13.1.** All information security incidents or other suspected breaches of this system are reported immediately to the ISO. For the escalation and reporting of data breaches that involve personal data, follow the Data Breach and Information Security Incident Reporting Procedure as described in ISMS.

**6.13.2.** Information security incidents will be investigated in accordance with the Security incident procedures to determine whether any underlying security concern need to be recorded, corrected and built into future controls. If appropriate, concerns will be added to the IT&IS risk register and reported to the IT&IS Leadership Team.

### 6.14. Information security aspects of business continuity management

**6.14.1.** DDF will protect critical IT services from the impact of major incidents to ensure recovery in line with documented priorities. This includes appropriate backup and resilience. Business continuity plans are maintained and tested. Business impact analysis is undertaken of the consequences of major security incidents.

### 6.15. Compliance

**6.15.1.** Compliance with the controls in this policy is monitored by the ISO and reported to the ISMSC.

**6.15.2.** The design, operation and use of IT systems must comply with all contracts and regulations, relevant to the Netherlands and EU laws. In brief this includes the General Data Protection Regulation, ISO/IEC 27001, and DDF contractual commitments.

**6.15.3.** DDF is subject to independent audit and aims to comply with the spirit of ISO/IEC 27001 and the EU Governments Cyber Essentials scheme. Business critical systems and other systems identified as high risk will be subject to regular penetration testing.

## 6.16. Appendix A |ISMS related DDF's Policies

### PART A | Governance, Legal Framework & Info Classification

[ISM.PL.A.00] | GENERAL INFORMATION SECURITY POLICY
[ISM.PL.A.01] | GOVERNANCE
[ISM.PL.A.02] | REGULATORY REQUIREMENTS AND LEGAL FRAMEWORK
[ISM.PL.A.03] | CLASSIFICATION OF INFORMATION

### PART B | Securing the End User

[ISM.PL.B.01] | ACCEPTABLE USE OF INFORMATION SYSTEMS
[ISM.PL.B.02] | BRING YOUR OWN DEVICE (BYOD) POLICY
[ISM.PL.B.03] | ACCESS CONTROL

### Part C | Securing the Network

[ISM.PL.C.01] | NETWORK AND COMMUNICATION SECURITY
[ISM.PL.C.02] | NETWORK TRAFFIC AND ACCESS CONTROL

### PART D | Securing the Systems

[ISM.PL.D.01] | SYSTEM SECURITY
[ISM.PL.D.02] | PROTECTION FROM MALICIOUS SOFTWARE
[ISM.PL.D.03] | SUPPLY, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS
[ISM.PL.D.04] | THIRD PARTIES SECURITY MANAGEMENT

### PART E | Physical Security

[ISM.PL.E.01] | PHYSICAL SECURITY

### PART F | Cybersecurity and Incident Response

[ISM.PL.F.01] | MANAGEMENT OF SECURITY INCIDENTS
[ISM.PL.F.02] | SECURITY INCIDENTS RECORDING AND LOGS
[ISM.PL.F.03] | REPORTING INFORMATION SECURITY INCIDENTS
[ISM.PL.F.04] | REPORTING INFORMATION SECURITY INCIDENTS TO OUTSIDE AUTHORITIES

### Part G | Business Continuity and Risk Management

[ISM.PL.G.01] | BUSINESS CONTINUITY MANAGEMENT
[ISM.PL.G.02] | PERIODIC INSPECTION
[ISM.PL.G.03] | SECURITY BACKUP COPIES
[ISM.PL.G.04] | RISK ASSESSMENT AND RISK MANAGEMENT

### 6.17. Appendix B |Interested Parties

The organization recognizes the following stakeholders as interested parties, as well as their relevant needs and expectations regarding the Information Security Management System

| Interested Parties | Needs & Expectations |
|---|---|
| **Board of Directors** | ▪ Good external image of the organization<br>▪ Fame<br>▪ Advantages over competition |
| **Employees and External Partners** | ▪ Trust in the safe handling of their personal information in their relationships with the organization<br>▪ Feeling like they're working with an organization that stands out from the competition |
| **Operators-(Customers)and Users (Third Parties)** | ▪ Trust in the safe handling of their information in their relations with the organisation<br>▪ Feeling that they ensure cooperation with an organization that stands out from the competition |
| **Suppliers of goods - Service providers** | ▪ Achieving mutual benefit<br>▪ Feeling that they ensure cooperation with an organization that stands out from the competition |
| **State** | ▪ Compliance with legal framework (personal data, communications privacy, intellectual property, etc.) |

### 6.18. Appendix C | Information Security and Data Privacy Management System

| Information Security and Data Privacy Management System (ISDPMS) | |
|---|---|
| | |
| **Information Security Management System (ISMS)** | **Privacy & GDPR Compliance Management System** |
| The ISMS includes policies and additional components, such as control points, procedures, forms and reports governed by a set of key principles that should be followed 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:<br>▪ ensure the confidentiality, integrity and availability of information,<br>▪ give equal treatment to all users of DDF for application, systems, technology, data,<br>▪ implement all the necessary measures to ensure the confidentiality and privacy of sensitive information collected from patients (or others) by DDF systems and also users who process such data. | The Privacy & GDPR Compliance Management System objective is to protect the subjects privacy also to exercise their rights |
| consists of<br>▪ Governance<br>▪ Roles Definitions<br>▪ Policies<br>▪ Procedures<br>▪ Forms<br>▪ Records | consists of<br>▪ Roles<br>▪ Privacy Policy<br>▪ GDPR Compliance<br>▪ DPIAs & Measures<br>▪ the ISMS (Supported by) |
| | |

This page is left intentionally blank

End of Document