An Phríomh-Oifig Staidrimh
Central Statistics Office

Data Management Policy Summary

Management Summary

Section 1 – Purpose, Scope and Legislation (Chapters 1 – 3)

This section details and defines the purpose and scope of the document, and the legislative context. The policy applies to all information systems and data (including paper records), employees and contractors and it confirms that the CSO is obliged to abide by all relevant Irish legislation and European legislation.

Section 2 – Working from home/working in a blended environment (Chapter 4)

This section sets out advice to all staff on working from home/working in a blended environment. The policy applies to all workplaces, be that the Office, a staff member's home or elsewhere and is based on advice published by the Data Protection Commissioner

Section 3 – Roles and Responsibilities (Chapter 5)

This section defines roles and responsibilities applicable to governance structures, management duties, policy and security support and the duties of staff at all levels in the CSO and third-party contractors.

Section 4 – CSO Data Classification Scheme (Chapter 6 and Annex A)

The data classification scheme and matrix (set out in Annex A) defines categories (and sub-categories) of data and set out detailed rules on the treatment of data. The classification was introduced in Office Notice 24/2014. This section and matrix describe the fundamental framework for how data and information should be processed in line with the CSO's legal obligations.

Section 5 – Data Protection (Chapter 7)

This section outlines principles of data protection, procedures for handlings data subject access requests, procedures for reporting and management of data security breaches as well as procedures required for contracts with processors.

7.1 Data Protection outlines the scope and principles of data protection and states the aim of the CSO to be fully compliant with the GDPR. It details the principles of data protection covering lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability.

7.2 Data Subject Access Requests (DSAR) sets out the procedures for handling data subject access requests (DSARs) in the CSO. Applications for access will be assessed on a case-by-case basis, however it is the intention of the Office to vindicate this right wherever possible.

7.3 Policy on Reporting and Management of Data Security Breaches sets out the procedures applicable to reporting and management of data security breaches, details how data security breaches are to be handled in the Office, the obligations of staff members to report them, the roles and responsibilities of designated staff and the timelines to be followed. It deals with the steps to be taken if a breach occurs and it applies to all CSO employees, service providers, contractors and third parties that access, use, store or process information on behalf of the Office. It states that safeguarding against and preventing security breaches is essential to maintaining the public's trust in the CSO. It also includes separately the procedures applicable to reporting and management of RMF Policy breaches.

7.4 Contracts with Processors details the arrangements for engaging processors to ensure that the processing will meet the requirements of the GDPR and ensures the protection of the rights of data subjects. A full written contractual arrangement must be put in place with all data processors to provide assurance that all applicable statistical confidentiality, data protection and data/information security standards are satisfied.

7.5 Data Handling Procedures sets out the arrangements for ensuring that CSO data is properly treated in line with the data classification policy and matrix, whether being transmitted within the organisation or to a trusted third party.

Section 6 – Policies (Chapters 8.1 – 8.14)

Chapter 7 articulates the various CSO policies that operate under the aegis of the overall Data Management Policy.

8.1 User Access Management (internal) describes the process of assigning new users, handling movers and removing leavers from all CSO information systems and services by Technology on the basis of an instruction from HRM and information from the supervisor. Access to systems is restricted to the user's business requirements; the purpose is to prevent unauthorised access to the Office's information systems and data.

8.2 Password Security Policy outlines the minimum mandatory password standards required for Information Systems within the CSO with certain elements relevant to Technology staff only. Locally managed systems may have more restrictive requirements and these may be adopted at the discretion of the local management. All CSO information systems must be protected by a username and password. All users must have individual passwords. It encompasses all information systems, desktop computers, laptops and tablets inside and outside the office and incorporates sections on complex passwords and password changes, transmission, misuse or compromise.

8.3 Data Retention and Destruction Policy outlines the arrangements for data retention and destruction in conjunction with Office Notices 09/2009 and 10/2016.

8.4 Data Archiving/Long term storage Policy describes the data archiving/long term storage policy in conjunction with section 8.3

8.5 Data Backup and Restore Policy describes the back and restore arrangements for the Office's three sites.

8.6 Laptop/Tablet Security Policy outlines the minimum mandatory standards required for use of Information Systems within the Office for Technology staff and those users who have access to CSO laptops/tablets with certain elements relevant to Technology staff only. Locally managed systems may have more restrictive requirements and these may be adopted at the discretion of the local management. It covers physical and IT security arrangements for laptops and tablets inside and outside the office including anti-virus, firewall protection and encryption.

8.7 Physical Security outlines the arrangements for staff access to CSO premises and managing the attendance of visitors and contractors at CSO premises in conjunction with Office Notices 10/2019 and 11/2019.

8.8 Redaction This section briefly describes the procedure for redaction (i.e. blackening out or deletion of text in a document) in the Office. The Data Office should be consulted first before preparing or issuing a redacted document

8.9 Administrative Data Governance & Analysis Policy sets out data governance procedures in the CSO's Administrative Data Governance & Analysis Centre unit, and details CSO users' access procedures and responsibilities concerning data holdings in the Administrative Data Governance & Analysis Centre data warehouse. This chapter stipulates that the details are set out in the ADGA Policy. The purpose of the reference is to bring the ADGA policy under the governance of the DMP. An Exceptions Register to the policy is maintained by Data Office.

8.10 Research Microdata Files (RMFs) prescribes the arrangements for managing access to RMFs by researchers and others under Section 20(c) of the Statistics Act 1993. These are unit record files provided for statistical research purposes by the Central Statistics Office (CSO) under Section 20(c) of the Statistics Act, 1993; they are not published or made available to the general public. The processes for authorising access to RMFs and for managing RMF research projects are strictly controlled by the CSO because of risk of disclosure through indirect identification. The purpose of the reference is to bring the RMF policy under the governance of the DMP.

8.11 Cryptography describes the cryptography solutions available to the Office and the key management procedures attaching to each approved product and the circumstances in which it should be used. It applies to all staff who use encryption.

8.12 Hand-over Procedures and Responsibilities outlines the formal procedures to be followed when work responsibilities are transferred from one area to another to provide the new area with key knowledge and information regarding the task(s) associated with the data and to prevent that data being lost.

8.13 Statistical Disclosure Control (SDC) for microdata provides guidance on the application of Statistical Disclosure Control (SDC) for microdata. It applies to all statistical areas providing microdata to appointed Officers of Statistics, as defined under Sections 20(b) and 20(c) of the Statistics Act, 1993. It does not prescribe specific methods of SDC to be used. However, statistical areas are required to document and retain the rationale for the SDC methods that have been applied.

8.14 Statistical Disclosure Control (SDC) for Tabular Data provides guidance on the application of Statistical Disclosure Control (SDC) for Tabular Data. The guidance applies to all staff compiling statistical tabular output. It does not prescribe specific methods of SDC to be used. However, statistical areas are required to document and retain the rationale for the SDC methods that have been applied.

Section 7 – Management and Governance (Chapters 9-13)

This section outlines enforcement, training, exceptions, monitoring and compliance of this policy, as well as reviews of the DMP.

9 **Enforcement** deals with enforcement procedures where there is a breach of the policy, highlighting that the Office reserves the right to take such action as it deems appropriate against users who breach the conditions of the policy. Users include CSO staff, Contractors and Other parties.

10 **Training** stipulates that appropriate training awareness will be provided.

11 **Exceptions** sets out that any exceptions to the DMP will require the authorisation of the CDSC. Exceptions are to be managed by the Head of the Data Office in conjunction with the Data Protection Officer (DPO), the administrative area concerned and/or Technology to determine the risk involved. An exceptions register is maintained by the Head of the Data Office.

12 **Monitoring and Compliance** set out that Technology is responsible for the monitoring of network activity. Any suspect behaviour must be reported to the IT Security Officer.

13 **Review and Updates to Policy** will be reviewed annually by the CDSC with additions and changes made as appropriate between reviews.

Section 8 – Appendices

Appendices 14.1, 14.2 and 14.3 sets out forms associated with 7.3 Policy on Reporting and Management of Data Security Breaches while Appendix 14.4 sets out a form associated with 8.12 Work Hand-over Procedures and Responsibilities.

Section 9 – Annexes

Annex A sets out the CSO data classification matrix while Annex B provides definitions for specific terms used in the policy.