CAN/DGSI 100-10 / HRSO 300.03

NATIONAL STANDARD OF CANADA

First Edition

2025-09

Data Governance in Human Research

03.100.02 03.100.40 35.020 35.030

HRSO
Human Research Standards Organization

SCC CCN

Table of Contents

Foreword **3**

Technical Committee **5**

Introduction **6**

1. Scope **7**

2. Normative References **8**

2.1 Canadian Legislation *8*

2.2 Canadian Regulations *8*

2.3 Policies and Guidelines *9*

2.4 National Standards of Canada and Global Standards *9*

2.5 Other Regulations *9*

3. Terms and Definitions **10**

4. Technical Requirements **14**

4.1 Authority, Accountability, and Responsibility *14*

4.2 Maintaining a Registry of Data Assets *16*

4.3 Data Management Plans (DMPs) *17*

4.4 Data Access *18*

4.5 Data Systems Validation *20*

4.6 Data Quality *20*

4.7 Compliance and Quality Improvement *21*

4.8 Privacy and Security Controls *21*

Informative Annexes **25**

Annex A: Informative References *26*

Annex B: Examples of Research Data Lifecycles (Informative) *27*

Annex C: Baseline Security Controls (Informative) *28*

Foreword

The Digital Governance Standards Institute (DGSI) develops digital technology governance standards fit for global use. The Institute works with experts, as well as national and global partners and the public to develop national standards that reduce risk to Canadians and Canadian organizations adopting and using innovative digital technologies in today's digital economy.

DGSI standards are developed in accordance with the *Requirements & Guidance – Accreditation of Standards Development Organizations*, 2019-06-13, established by the Standards Council of Canada (SCC).

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. DGSI shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of this Standard are included in the Introduction.

For further information about DGSI, please contact:

Digital Governance Standards Institute
500-1000 Innovation Dr.
Ottawa, ON K2K 3E7
www.dgc-cgn.org

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca .

HRSO is a Canadian, not-for-profit, standards development organization that develops standards of relevance to Canadians conducting, overseeing, and participating in human research.

Human research standards ensure that the rights and welfare of Research Participants are safeguarded, and that human research is conducted in an environment that promotes efficiencies, mitigates risks, and produces reliable, verifiable, and credible data. The adoption of standards for human research ensures harmonization, partnership, and economic growth of this activity within Canada and internationally.

HRSO adheres to the World Trade Organization (WTO) Agreement on Technical Barriers to Trade: Code of Good Practice for the Preparation, Adoption, and Application of Standards in the development of service and management standards for human research.

The timeline for development of NSC CAN/DGSI 100-10 / HRSO 300.03 Data Governance in Human Research was as follows:

Notice of Intent Publication: 2022/10/20
First Meeting of Technical Committee: 2023/03/16
Public Consultation Period: 2025/01/23 – 2025/03/28
Final Meeting of Technical Committee: 2025/06/19
Publication of First Edition: 2025/09/11

All units of measurement expressed in this Standard are in SI units using the International system (SI).

This Standard is subject to technical committee review beginning no later than two years from the date of publication. The completion of the review may result in a new edition, revision, reaffirmation or withdrawal of the Standard.

The intended primary application of this Standard is stated in its scope. It is important to note that it remains the responsibility of the user of the Standard to judge its suitability for a particular application.

This Standard is intended to be used for conformity assessment.

ICS:
03.100.02 03.100.40 35.020 35.030

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE.

Technical Committee

Members and Contributors

Clarissa Alberti Fleck, BSc; Quebec

Sassan Azad, BSc, MSc; Ontario

Alexander Bernier, BCL, JD, LLM, SJD; Quebec

Andria Bianchi, BA, MA, PhD; Ontario

Shamir Charania, BEng; Alberta

Liseanne Cadieux, BS, BASc, MIS; Nova Scotia

Colleen Cochran, BA; Saskatchewan

Natalie Comeau, BA, MHSc; Ontario

Sean Gowing, CISSP; Alberta

Kiren Handa, BSc, MSc, MBA; Ontario

Courtney Heisler, BSc, MSc; Nova Scotia

Cassie Hill, BA, MHA; Nova Scotia

Karey Iron, BA, MHSc, CIPM; Ontario

Alexander Karabanow, BSc, BAA; Ontario

Tatiana Kawakami, BA, MBA, MBA; British Columbia

Jude Dzevela Kong, BEd, BSc, MSc, PhD; Ontario

Diana Kulpa, BA, MA; Ontario

Michael McDonald, BA, MA, PhD; British Columbia

Erica Monteferrante, BA, MA; Quebec

Waqar Mughal, BSc, MSc; Ontario

Janice E. Parente, BSc, PhD; Quebec

Dimitri Patrinos, BSc, LLB, JD, LLM; Quebec

Mikayla Redden, BA, MLIS; Ontario

Katie Roposa, BScN, MEd, RN; Ontario

Eric Sutherland, BMath, MMath; Ontario

Kristi Thompson, BA, MLIS; Ontario

Marie-Laurence, Tremblay, BSc, PhD; Nova Scotia

Jeffrey Webster, BSc, MEnvSc; Ontario

Donald Willison, BSc, MSc, ScD; Ontario

Lee Wilson, BA, MLIS; Nova Scotia

Standards Officers

Martin Letendre, BA, LLB, LLM; Quebec (HRSO)

Darryl Kingston, BA; Ontario (DGSI)

Cherlene Tay, BComm; Ontario (DGSI)

Introduction

Data governance in human research serves several purposes. It optimizes research data use to meet the needs of the Research Enterprise (RE, such as an institution or corporation that, as part or all of its activities conducts or facilitates human research) and ensures that the use of research data meets ethics and legal obligations, and it applies safeguards to ensure appropriate access and protection against data corruption or other misadventure. When good data governance is demonstrated, it generates trust among all parties, including Research Participants, that research data are being used responsibly and in the public interest.

Increasingly, research sponsors and publishers require that Investigators/Researchers make their research data more broadly available at the conclusion of the research. This places an onus on the RE and the Investigators/Researchers to consider the implications of data sharing on data governance throughout the lifecycle of the research data, such as:

- during the planning of the study;
- at the point of data collection (ensuring that Investigators/Researchers address data disposition and future re-use of research data in the informed consent process);
- data processing (ensuring that metadata records are sufficiently complete and informative for any secondary user); and
- data storage and archiving (appropriate storage of the data, ensuring that the relevant data are discoverable, and processes are in place to adjudicate and process external data requests).

See Annex B for examples of research data lifecycles.

As research data are increasingly collected, processed, and stored digitally, risks arising from both deliberate and unintentional actions have more significant effects due to the unique properties of digital data. For example, digital data are subject to various risk of harm, as they can be copied near instantaneously across the world. Thus, the governance of people, processes, systems and third parties that handle data is important. A particular concern is the potential for personal information and information subject to intellectual property rights to be exposed through theft, loss or unauthorized access, leading to identity theft, financial fraud, reputational damage or other harms to participating individuals, organizations or other groups. Weaknesses in software or

operating systems can be exploited by cybercriminals to gain unauthorized entry, through hacking, malware, and phishing attacks, which emphasizes the importance of regular updates and patches to technology. Additionally, the increasing availability of third-party services, including cloud storage, requires the clarification of roles, responsibilities, and the protections third parties will provide around data. Social engineering tactics, where attackers manipulate individuals into divulging confidential information, further contribute to the vulnerability of digital data to cyberattack. As technology evolves rapidly, continuous efforts are needed to stay ahead of potential vulnerabilities and safeguard digital assets.

The purpose of this NSC is to provide users, such as RE, Investigators/Researchers, and auditors, with tangible measures to assess the conduct of good data governance. It complements various normative texts, most notably the Tri-Agency Research Data Management Policy and the Tri-Council Policy Statement (TCPS2).

1. Scope

The NSC applies to all individuals engaged in the conduct of human research. It also applies to for-profit and not-for-profit, public, and private organizations. In this document, any entity that conducts or facilitates human research is called a Research Enterprise (RE). An RE may exist as a component of a larger institution (e.g., a university) or corporation, or as a component of a Human Research Protection Program (HRPP).

By reducing the variability of interpretation of regulations, policies, and guidelines, this NSC provides a basis for the establishment of unambiguous procedural documents that adhere to Canadian and international normative references.

Human research incorporates various types of qualitative and quantitative methods, disciplines (health, social sciences and humanities, arts, engineering), and approaches (interventional, observational) conducted in a variety of domains (biomedical, social, legal, behavioural). Human research may involve the use of existing or prospectively collected data, specimens, images, observations, or audio/video recordings, both digital and analog. This standard applies to all digitized and digital data.

Because of the diversity of research disciplines and methods, this NSC covers data governance issues, practices, and processes held in common and acknowledges where there may be discipline-specific requirements or norms with which the reader should conform.

For purposes of this NSC, human research use-case scenarios include but are not limited to:

1. Prospective data collection or generation to address a specific research question or engage in a specific research objective,
   (a) where there is no explicit plan to re-use the data, or
   (b) where the Investigator/Researcher anticipates that data may be re-used in future (by the same or different Investigators/Researchers), or
   (c) where the research sponsor requires that data be re-used in future.

2. Use of existing data to address a specific research question where these data,
   (a) were created for purposes other than research, or
   (b) were created for a research purpose with or without prior planning for secondary use.
3. Prospective data collection specifically for use in future unspecified research uses,
   (a) where data are being collected directly from the individual, such as, biobanks and registries, or
   (b) where the prospective collection consists of the collation of longitudinal data derived from existing data that were created for purposes other than research (e.g., administrative data), or
   (c) a hybrid of (a) and (b) above.
4. Creation of new data elements derived from existing data.

“Shall” vs “Should”

In this NSC, “shall” indicates that the requirement is mandatory and is supported by normative references, whereas “should” indicates that the requirement is recommended, or a best practice statement.

2. Normative References

This NSC was developed in accordance with the normative documents listed below, all of which are publicly available. The user of this NSC should refer to the latest edition or revision of the normative documents.

2.1 Canadian Legislation

Health Canada Food and Drugs Act https://laws-lois.justice.gc.ca/eng/acts/F-27/page-1.html

Personal Information Protection and Electronic Documents Act (PIPEDA) https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html

Office of the Privacy Commissioner of Canada: Provincial and Territorial Privacy Laws and Oversight https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

2.2 Canadian Regulations

Health Canada Food and Drugs Regulations, Part C, Division 5 https://www.canada.ca/en/health-canada/services/drugs-health-products/compliance-enforcement/good-clinical-practices/guidance-documents/guidance-drugs-clinical-trials-human-subjects-gui-0100.html

Health Canada Natural Health Products Regulations, Part 4 https://laws-lois.justice.gc.ca/eng/regulations/SOR-2003-196/page-7.html

Health Canada Medical Device Regulations, Part 3 https://laws-lois.justice.gc.ca/eng/regulations/sor-98-282/page-9.html#h-1021976

2.3 Policies and Guidelines

Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans - TCPS 2 https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2022.html

Interpretations - Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans - TCPS 2 Interpretations https://ethics.gc.ca/eng/policy-politique_interpretations.html

Material Incidental Findings - Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans - TCPS 2 https://ethics.gc.ca/eng/incidental_findings.html

Tri-Agency Research Data Management Policy https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97610.html

International Council for Harmonization (ICH) of Technical Requirements for Pharmaceuticals for Human Use Good Clinical Practice Guideline https://www.ich.org/page/efficacy-guidelines

Good Clinical Data Management Practices (GCDMP) https://scdm.org/gcdmp/

The First Nations Principles of Ownership, Control, Access, and Possession OCAP® https://fnigc.ca/ocap-training/

2.4 National Standards of Canada and Global Standards

CAN/DGSI 104:2021 / Rev 1: 2024 Baseline Cybersecurity Controls for Small and Medium Organizations https://dgc-cgn.org/product/can-dgsi-1042021-rev-12024/

CAN/DGSI 129 / HRSO 100.01/ Rev 1:2024 Development of a Human Research Protection Program (HRPP) https://www.hrso-onrh.org/standards/published-standards/

CAN/HRSO-200.01-2021 Ethical Review and Oversight of Human Research https://www.hrso-onrh.org/standards/published-standards/

CAN/HRSO-300.01-2022 Conduct of Human Research https://www.hrso-onrh.org/standards/published-standards/

HRSO-100.02-2023 Development of a Training Program for Human Research Protection https://www.hrso-onrh.org/standards/published-standards/

ISO/IEC 27000:2018-02 Information technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

2.5 Other Regulations

US Code of Federal Regulations Title 21 https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm

US Code of Federal Regulations Title 45 https://www.ecfr.gov/current/title-45

General Data Protection Regulation https://gdpr.eu/tag/gdpr/

3. Terms and Definitions

Biological Materials: This term includes tissues, organs, blood, plasma, skin, serum, DNA, RNA, proteins, cells, hair, nail clippings, urine, saliva, and other body fluids. The term also includes materials related to human reproduction, including embryos, fetuses, fetal tissues and human reproductive materials.

Collective/Community Consent: An agreement that is achieved through adherence to the governance structure of the Community in question. In the absence of a governance structure, an agreement is achieved through consultation with groups of individuals reflecting the diversity of the Community in question.

Collective or Group Rights: Ethical or legal rights held by groups in contrast to rights held by individuals. Collective right holders include corporations, voluntary associations, and Communities. These are groups with shared interests, mutual recognition of membership responsibilities, formal or informal governance structures, and often a common heritage and traditions. Such rights establish domains of sovereign control and governance. When the Population Under Study is a group with collective rights, it must play a role in the governance of the research.

- **Collective Rights of Indigenous Peoples:** These are collective rights that belong to Indigenous Peoples around the world (see UNDRIP) and are embedded in Canadian law and in local Indigenous laws and customs. These rights affirm Indigenous sovereignty, control of land, resources, and access to the Community.

Community: A group of people with a shared identity or interest that has the capacity to act or express itself as a collective. A Community may be territorial, organizational, or defined by a shared interest. A Community may have governance processes that affect human research such as leadership engagement, recruitment, consent, and dissemination and ownership of research results.

Community and Research Participant Engagement: A process that establishes an interaction between an Investigator/Researcher, or a Research Team, and a Community or individual participants. It signifies the intent of forming a collaborative relationship between them with the goal of reciprocal accountability, although the degree of collaboration may vary depending on the Community context and the nature of the research.

Conflicts of Interest: A set of conditions or factors (such as money, friendship, reputation) in which professional judgment concerning a primary interest (such as the welfare of a Research Participant) is unduly influenced or is reasonably perceived to be so influenced by a secondary interest (such as financial gain). Conflicts of interest have the following components:

- a relationship - one party (the trustor) is entitled to trust that the other (the trustee) will promote or protect their interests in relation to matters within that relationship.

- a conflicting interest - an influence that tends to make the trustee's judgment on a given decision less reliable in promoting or protecting the trustor's interests than it would normally be.
- an exercise of judgment - the trustee must be able to make a decision that affects the trustor's interests.

Conflicts of Roles: A situation that occurs when incompatible demands are placed on an individual relating to their job or position, such as conflicting fiduciary responsibilities (e.g., an Investigator/Researcher reviewing their own research while serving on an REB).

Conformity Assessment: Processes used to demonstrate that a product, service, management system or body meets specified procedures or requirements.

Data: Any set of values of qualitative or quantitative variables. Data may be recorded in any format (e.g., electronic, paper) and include *de novo* collections or secondary use of existing data.

Data Access: Open, registered, controlled, and private data access are defined below.

- Open access: Data is shared with the public without restricting the categories of users that can access the data, nor imposing significant limitations on the acceptable purposes of data use.
- Registered access: Data is made directly available to all users that create an account or otherwise ask for access to the data, and that assert compliance with applicable policies on responsible data use.
- Controlled access: Data is made available to authenticated users that submit to a rigorous application process that often includes signing binding data access agreements, review of the intended data uses by an expert committee or oversight body, and demonstration of research credentials and affiliation to a recognized research organisation on the part of the applicant.
- Private access: Data that cannot be shared outside of the organisation that generated it or that otherwise holds it, for third parties to use for their own research purposes.

Data Asset: Any structured or unstructured collection of digital information that has value to an organization or individual.

Data Custodian/Steward/Owner: The party (person or organization) that has been selected as custodian of the data, i.e., responsible for managing the associated protection sphere. A Data Custodian is responsible for developing and maintaining all applicable safeguards.

Data Governance: There are many definitions of data governance. Below are two definitions to provide a sense of some of the nuances:

- The exercise of authority, control, and shared decision making (planning, monitoring, and enforcement) over the management of data assets (Ladley, 2020).
- How an organization maintains security, complies with regulations and laws, and meets ethical standards when managing information (Smallwood, 2019).

Data Management Plan (DMP): A project-specific document that outlines the strategies, practices, and processes for managing data throughout the entire research lifecycle, including the active, repository and archive/destruction phases. A DMP must evolve alongside the project and be regularly updated to reflect changes in design, methodology, or data-related requirements, ensuring responsible and effective data curation and management from inception to completion and beyond.

Data Sovereignty: Generally referring to data control, management, and governance consistent with laws, practices, and customs of the jurisdiction in which it is located, generated or processed.

- **Indigenous Data Sovereignty (IDSov):** Indigenous Peoples, whose knowledge systems predate current colonial arrangements, have their own information governance structures. In this context, data sovereignty is defined as the right of Indigenous Peoples to collect, analyze, interpret, manage, distribute, and reuse all data that derived from or related to their communities. Sovereignty extends to traditional knowledge and digitized data.

Documented Procedures: A collective term used to describe policies, procedures (such as standard operating procedures), and guidelines.

Human Research: A systematic, rigorous investigation involving human beings that includes, but is not limited to, the following disciplines: health research, social sciences and humanities research, creative and arts-based research, and engineering research, and includes, but is not limited to, the following methods:

- interventional research, observational research
- qualitative research, quantitative research
- social and behavioural research, health services research, public health research, educational research
- research involving existing human data and human biological materials and their derivatives
- research involving living or deceased individuals.

Human Research Protection Program (HRPP): An organization-wide program composed of a network of interdependent entities that share the responsibility for Research Participant protection and interact in a system that promotes a culture of research integrity, quality, efficiency, accountability, and evidenced-based practices. A HRPP can exist in any for-profit or not-for-profit, public or private organization where human research is conducted and/or overseen.

Identifiable Research Data: Information that may be reasonably expected to identify an individual, alone or in combination with other available information. Also referred to as personal information.

Indigenous Peoples: In the context of Canada, persons of First Nations, Inuit, or Métis descent, regardless of where they reside and whether their names appear on the Canadian government register, or other Provincial, Territorial, or regional arrangements.

Informed Consent: The free, voluntary, informed, and ongoing agreement by an individual to become a participant in research.

Individuals who Play a Role in the RE: Any individual or entity within an organization whose actions directly or indirectly affect research data integrity and the welfare, interests, or rights of Research Participants, such as Investigators/Researchers, Administrative Personnel, Student Researchers, Research Coordinators, Research Monitors, Research Associates, and Community or Patient Partners

Investigator/Researcher: In the context of a RE or HRPP, an individual who carries out human research.

Metadata: Data that provide context for the data collected. Originating from bibliographic records about books, metadata increases the findability and useability of data and makes it more manageable. Metadata is often larger than the data it is contextualising. It may be descriptive (provide characteristics about the data, its creator, Custodian, Steward or Owner) structural (describe the organizational structure of the data), or administrative (indicates the origin of the data, its type, and the rights and limitations to access it).

National Standard of Canada (NSC): A standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC.

Population Under Study: A well-defined population identified as the subject of the research, for example, a population having a common physiological, psychological, or social condition. In some research, the population identified has collective rights affecting access to and control of data from the population in question.

Privacy: The right of individuals to determine for themselves what information about them is collected, accessed, used, shared, stored, and destroyed, and by whom and to whom that information may be disclosed.

Research Data: Data used for research purposes. For the purpose of this NSC, the term “research data” is restricted to data about humans, including their biological materials.

Research Enterprise (RE): An entity, such as an institution or corporation that, as part or all of its activities, conducts or facilitates human research. A RE can exist as a component of a HRPP.

Research Ethics Board (REB): An appropriately constituted group that applies ethics principles in its review and ongoing evaluation of research involving humans. An REB is also known as an independent or institutional review board (IRB), independent ethics committee (IEC), a research ethics review committee (RERC), a research ethics committee (REC), or ethics review board (ERB).

Research Participant: An individual whose data, biological materials, or responses to interventions, stimuli, or questions may be used to answer one or more research questions.

Research Team: A group of individuals working together in a committed way towards a common research goal.

Secondary Use: The use of data or human biological materials for a purpose other than the original purpose for which it was collected.

Systems Validation: A structured process to verify that an entire system meets pre-established requirements and parameters to ensure that the system functions in specific circumstances. Systems Validation includes hardware, software, and network elements.

Traditional Knowledge: Information that is transmitted between generations including languages, stories, ceremonies, dance, song, arts, hunting, trapping, gathering, food and medicine preparation and storage, spirituality, beliefs, and world views. Traditional Knowledge is one form of Indigenous Peoples' data.

Vendors and Sub-Contractors: Entities that sell products and services to the RE or HRPP (Vendors) or provide services under contract to the RE or HRPP (Sub-Contractors). Some important examples of Sub-Contractors include, but are not limited to, external REBs, external Investigators/Researchers, external biobanks, and contract research organizations.

4. Technical Requirements

This NSC describes the policies, processes, people, and infrastructure required to support data governance capabilities at the level of the RE. The exercise of data governance varies across REs depending on the degree of centralization of decision-making and accountability. For example, accountability for the use of research data may be much less centralized in a university setting than in a corporate setting. These contextual factors promote innovative accountability structures and harmonization of policies and procedures that govern research data across collaborating REs, the elements of which are described below.

4.1 Authority, Accountability, and Responsibility

4.1.1 The RE shall have documented procedures consistent with the relevant laws, normative texts, and NSCs governing its collection, storage, use, and sharing of data concerning human Research Participants. These laws, normative texts, and NSCs are usually identified by the highest authority in the institution or organization in which the RE operates and are included in the RE's mandate (see NSC CAN/HRSO-300.01-2022 Conduct of Human Research, section 4.1.1 "Mandate").

4.1.2 The RE shall conduct research in conformity with NSC CAN/HRSO-300.01-2022 Conduct of Human Research.

4.1.3 The RE shall have documented procedures for ensuring continued resources to provide privacy and security management of the research data throughout its lifecycle in accordance with this standard. The level of support must be in proportion to the size and complexity of the research conducted and include funding, qualified personnel, space, equipment, materials and technology.

4.1.4 The RE shall have documented procedures for identifying and documenting the delegated responsibility and authority (including position descriptions) for the management of research data assets in its custody over the lifecycle of the research data. Activities associated with managing the research data assets for

which authority and responsibility need to be assigned include, but are not limited to:

(a) maintaining a registry of data assets in the custody of the RE (see section 4.2);

(b) curating relevant data classification systems to ensure that all research data under the purview of the RE are classified appropriately. This may involve identifying a number of classification systems to support the needs of the diverse types of research carried out within the RE (see section 4.2.2);

(c) supporting the development and maintenance of Data Management Plans (DMPs) in the RE (see section 4.3);

(d) defining, maintaining, and monitoring research data quality standards addressing accuracy, completeness, consistency, immutability, integrity, reliability, and timeliness, where required (see section 4.6).

(e) monitoring and facilitating compliance with relevant laws, normative texts, and NSCs (see section 4.7);

(f) providing secure data collection modalities, computing environments, and other solutions to support research activities across the data management lifecycle (see section 4.8); and

(g) defining, maintaining, and monitoring appropriate authorized and justified access to the research data at specific points in the data lifecycle (see section 4.4), such as:

- the active phase when research data are being collected, processed, and analyzed,
- the repository phase for purposes of facilitating access to other Investigators/Researchers, if applicable,
- the archive/destruction phase for purposes of long-term archiving or secure destruction of research data, if applicable.

4.1.5 The RE shall have documented procedures that specify:

(a) who retains custody over any research data collected should the lead Investigator/Researcher cease to participate in the RE;

(b) the disposition and governance of the research data should the RE cease operations or change ownership; and

(c) if the research involves an Indigenous Community, how the RE upholds and respects Indigenous sovereignty over the data including access, ownership, and control of the research data.

4.1.6 The RE shall have documented procedures for maintaining and mandating the use of computing systems to act as the system of record for all policy/process documents. (See capability requirements: 4.8.7 (b), (k), (n).)

4.2 Maintaining a Registry of Data Assets

The RE shall have documented procedures for maintaining a registry of data assets. Elements of the registry should be made available to the public to foster transparency and innovation through open science.

4.2.1 The RE shall have documented procedures for maintaining a registry that includes, at a minimum, the following for each data asset:

(a) a clear description of the subject matter;

(b) the variables included;

(c) the data classification system used (see section 4.2.2);

(d) the start and end dates of research data collection;

(e) the data sources for both primary data collection and secondary use of existing data assets;

(f) the location of the corresponding project-specific DMP;

(g) contact information for named individual(s) or committee(s) accountable for the data asset (e.g., Data Custodian/Steward, legal officer, Investigator/Researcher);

(h) the phase in the data lifecycle (active, repository, archive/destruction);

(i) when the data was locked (i.e. no longer able to be modified or manipulated), if applicable;

(j) the data expiry date;

(k) the data destruction plan and, once conducted, evidence that the destruction has occurred;

(l) a record of those internal staff who have been granted access to the data and for what purposes, such as: to create, read, update, and delete research data as well as share or provide download access; and

(m) a record of those external to the original project who have been granted access to or to whom data have been disclosed for specific purposes (such as multi-centred studies, secondary analyses, assistance in specialized aspects of the research, or as a part of open-access publishing).

4.2.2 The RE shall have documented procedures for classifying the data, including, but not limited to, the following criteria:

(a) research discipline (such as health, life-sciences, social sciences, humanities, arts, natural sciences, engineering, with appropriate sub-classifications);

(b) characteristics of the Population Under Study (such as sociodemographic, geographic, health, vulnerability, community membership);

(c) research design (such as quantitative, qualitative, or mixed methods; experimental or observational; exploratory or explanatory research); and

(d) sensitivity of data (such as individual or aggregate).

4.2.3 The RE should have documented procedures for publicizing the registry of data assets, along with the name and coordinates for the person to contact for further inquiry about the data assets.

4.2.4 The RE should have documented procedures for maintaining a record of enquiries about the data assets, including general inquiries and requests for access. Where the enquiry results in a request for access to or disclosure of the data asset(s), then the RE should record the contact information and nature of the access or disclosure.

4.2.5 The RE shall have documented procedures for maintaining and mandating the use of computing systems to act as the system of record for all data registry data and related processes. (See capability requirements: 4.8.7 (b), (k), (n).)

4.2.6 The RE shall have documented procedures for providing and maintaining a service catalogue with a comprehensive inventory of services including its purpose, features, and requirements. The service catalogue should facilitate easy access, searchability and include mechanisms for service and access requests.

4.3 Data Management Plans (DMPs)

4.3.1 The RE shall have documented procedures for supporting Investigators/Researchers in the development and maintenance of DMPs for each research project, including but not limited to:

(a) providing templates and other guidance to inform the development, maintenance, and updating of project specific DMPs, according to best practices and normative references, including but not limited to the following elements:

- a clear articulation of the research objective or research question;
- the specification of the data and the corresponding metadata required;
- measures undertaken to ensure consistent and accurate metadata are captured and updated across the project lifecycle;
- listing of data sources (such as Data Custodians) and the proposed methods and authority by which the data will be collected, used and disclosed;
- description of Research Participants and Population Under Study (such as individuals with a particular health condition, or residents of a particular geographic area);
- the parameters placed on use of the data, including re-use, and whether a record of the consent (including exemption of consent) is available;
- the methods that will be employed to perform an analysis of the research (i.e. analytic methods);
- the measures taken for the secure management of the data throughout the human research lifecycle (such as training of the Research Team and data security protocols);

- the measures undertaken to meet legal and ethical obligations pertaining to the collection, use, storage, sharing and publication of the data;
- the measures taken for continued data management (such as storage and quality maintenance);
- the roles and responsibilities of the Research Team members in relation to the data being collected and processed;
- confirmation that the project's budget includes provision for the continued implementation and maintenance of the DMP;
- key data-related issues encountered, and responses/decisions made over time;
- whether and how the data will be shared and re-used once the project is completed; and
- the measures taken to implement agreements for data contribution and access within or outside the RE (such as data use agreements, data sharing agreements, data contribution agreements, memoranda of understanding).

(b) providing a centralized location for storage of DMPs;

(c) storing and versioning of the DMPs in a non-repudiated way to permit an audit trail;

(d) establishing and maintaining a process to periodically review and update DMPs, such as annually, or as needed (e.g., when governing laws or data access and storage technologies change);

(e) ensuring maintenance of and compliance with DMPs, including the pathway for escalating issues; and

(f) maintaining a registry of completed DMPs.

4.3.2 The RE should have documented procedures to review and approve DMPs developed by Investigators/Researchers under its auspices.

4.3.3 The RE shall have documented procedures for maintaining and mandating the use of computing systems to act as the system of record for all Data Management Plans. (See capability requirements: 4.8.7 (b), (k), (n).)

4.4 Data Access

4.4.1 For lead Investigators/Researchers and their team, the RE shall have documented procedures for:

(a) determining to whom access to the data is granted, based on their roles and responsibilities, and for what purposes, such as creating, reading, updating, and deleting research data as well as sharing or providing download access;

(b) monitoring and recording who accesses the data and under what conditions data are accessed or used for specific purposes (such as multi-centred studies, secondary analyses or replication);

(c) determining for how long access to a research project's data is granted, including criteria for determining how frequently access privileges will be reviewed;

(d) ensuring that authorized personnel have timely and unrestricted access to the project data for the duration of the research project (such as clinical trials); and

(e) rescinding in whole or in part an individual's access privileges.

4.4.2 For external Investigators/Researchers, the RE shall have documented procedures for:

(a) determining to whom access to the data is granted, based on their roles and responsibilities, and for what purpose, such as creating, reading, updating, and deleting research data as well as sharing or providing download access;

(b) monitoring and recording who accesses the data and under what conditions data are accessed or used for specific purposes (such as multi-centred studies, secondary analyses or replication);

(c) determining for how long access to a research project's data has been granted, including criteria for determining how frequently access privileges will be reviewed;

(d) ensuring that external Investigators/Researchers have ready access to information (including metadata) about research data assets that are available for secondary analysis including the process for accessing them (See Section 4.1.2.3); and

(e) rescinding in whole or in part an individual's access privileges.

4.4.3 For Community Partners, the RE shall have documented procedures for:

(a) determining to whom access to the data, is granted, based on their roles and responsibilities, and for what purpose, such as creating, reading, updating, and deleting research data as well as sharing or providing download access;

(b) monitoring and recording who accesses the data and under what conditions data are accessed or used for specific purposes (such as multi-centred studies, secondary analyses or replication);

(c) determining for how long access to a research project's data has been granted, including criteria for determining how frequently access privileges will be reviewed; and

(d) rescinding in whole or in part an individual's access privileges.

4.4.4 For Research Participants, the RE shall have documented procedures describing the process for Research Participants to access their data based on consent, relevant laws, normative texts, and NSCs.

4.4.5 For Indigenous Peoples and Communities, the RE shall have documented procedures for ensuring that their data sovereignty is upheld, including a process for ensuring:

(a) their rights, interests and authority to own, access, and control their research data under relevant laws, practices, and customs of the region, including treaties, the United Nations Declaration on the Rights of Indigenous Peoples, and IDSov frameworks (e.g. CARE principles, Principles of OCAP®) are protected; and

(b) legal requirements and policies applicable to the RE do not unduly burden or restrict the authority of Indigenous Peoples and Communities to own, access, and control access to their research data.

4.4.6 The RE shall have documented procedures for maintaining and mandating the use of computing systems to act as the broker/mediator for data sharing and access. (See capability requirements: 4.8.7 (c), (f), (g), (i), (j).)

4.5 Data Systems Validation

The following requirements set out technical requirements for Data Systems Validation. NSC CAN/HRSO-300.01-2022 Conduct of Human Research, section 4.1.8 “Selection of Vendors and Sub-Contractors” shall apply to any procedures related to selection of Vendors and Sub-Contractors.

4.5.1 The RE shall have documented procedures for assessing and validating hardware and software for collecting and processing research data (such as systems to support informed consent, electronic data capture, electronic participant reported outcomes, wearables).

4.5.2 The RE shall have documented procedures for maintaining and making available to Investigators/Researchers a list of the hardware and software that have been validated by the RE after reviewing and accepting all risks related to fit for purpose (including availability and integrity of the functions provided), privacy, security and legal/contractual obligations.

4.5.3 The RE shall have documented procedures for maintaining the validation of previously validated hardware and software under section 4.5.2 above.

4.5.4 The RE shall have documented procedures for maintaining and mandating the use of computing systems to act as data capture for capturing data as part of research activities. (See capability requirements: 4.8.7 (h), (k), (m).)

4.6 Data Quality

4.6.1 The RE shall ensure that Investigators/Researchers have documented procedures to manage data across its lifecycle, such as:

- data accuracy
- data validity
- data traceability
- data completeness
- data uniqueness (non-redundant)
- data consistency.

4.6.2 The RE shall have documented procedures for maintaining and mandating the use of computing systems that store captured data. (See capability requirements: 4.8.7 (e), (n).)

4.7 Compliance and Quality Improvement

4.7.1 The RE shall have documented procedures for assessing and managing compliance of Investigators/Researchers, partners, third parties with its policies and procedures, ensuring that its procedures conform to relevant laws, normative texts, and NSCs (see NSC CAN/HRSO-300.01-2022 Conduct of Human Research, section 4.1.7 “Compliance and Quality Improvement”).

4.7.2 The RE shall have documented procedures for assessing the effectiveness of data governance outcomes across the data lifecycle.

4.7.3 The RE shall have documented procedures for:

(a) responding to incidents or suspected incidents of non-compliance (e.g. a breach of privacy) through investigation, containment, remediation, notification to affected parties, reporting to external parties to whom the RE has responsibilities, as applicable;

(b) investigating and mitigating areas of risk that threaten the ability to maintain compliance; and

(c) monitoring all real and suspected incidents.

4.8 Privacy and Security Controls

Because the task of secure data management has become so complex, accountability falls upon the RE for ensuring that Investigators/Researchers have private and secure environments for managing their research data. Data Security at the level of the RE consists of data security controls and capabilities.

4.8.1 The RE shall have documented procedures for resourcing and procuring dedicated and qualified personnel with expertise, experience, and authority to support, implement and manage privacy and security controls across all data assets and throughout the research data lifecycle, in proportion to the mandate of the RE (See 4.1.3; 4.1.4 (e), (f), (g); 4.4).

4.8.2 The RE shall have documented procedures for assessing requirements for data privacy and security training in proportion to the type of research being conducted. Requirements include but are not limited to:

(a) CAN/DGSI 104:2021/Rev1:2024 Baseline Cybersecurity Controls for Small and Medium Organizations, Clause 4.3;

(b) CAN/DGSI 118 Cybersecurity: Cyber Resiliency in Healthcare, Clause 5.

4.8.3 The RE shall have documented procedures for ensuring that individuals who directly or indirectly have access to the data across the data lifecycle:

(a) have a valid purpose to access the data that aligns with the REB-approved protocol, consent obtained for data use, and the governing DMP;

(b) have been thoroughly vetted, including relevant background checks;

(c) have signed documents with the RE concerning the non-disclosure of confidential information and a declaration of conflicts of interest and roles;

(d) are supervised and appropriately trained; and

(e) have controlled and monitored access to research data.

(See 4.4 Data Access and NSC CAN/HRSO-300.01-2022 Conduct of Human Research, section 4.1.2 “Qualifications and Training of Individuals who Play a Role in the RE”.)

4.8.4 The RE shall have documented procedures for providing and using private and secure environments, whether the secure environments are managed by the RE directly, have been outsourced to a third-party provider, or other contracted entity. If the RE is engaging third-party Vendors and Sub-Contractors to provide secure environments, see section 4.5 Data Systems Validation.

4.8.5 The RE shall have documented procedures that outline data privacy and security expertise and training requirements in proportion to the type of research being conducted in the organization and the role of the trainees.

4.8.6 The RE shall have documented procedures for assessing risks in their operational context at each stage in the data lifecycle. Risks to privacy and security of research data include, but are not limited to:

(a) data loss, theft, or corruption (from activities such as ransomware, industrial espionage);

(b) social engineering or similar attacks including phishing;

(c) unsecure communication or data transfer (such as failure to use a virtual private network or two-factor authentication); and

(d) accidental or intentional misuse of data by authorized individuals.

4.8.7 The RE shall have documented procedures for applying controls (such as physical, technical, and procedural controls) for the risks assessed under section 4.8.6. Controls to address risks to the privacy and security of the research data include, but are not limited to:

(a) requiring changing of default passwords;

(b) automated programs to detect weak or breached passwords;

(c) approved procedures for de-identification of identifiable research data;

(d) working areas management;

(e) workstation management;

(f) identity and access management; and

(g) ensuring that third-party service providers adhere to requirements.

4.8.8 The RE shall have documented procedures for deploying and managing its privacy and security capabilities. The security capabilities include, but are not limited to:

(a) a dedicated system for securely storing and managing sensitive information, such as passwords, API tokens, and database credentials;

(b) a digital signature system for obtaining verified digital signatures of participants;

(c) a system for managing consent obtained from participants;

(d) a process management capability to facilitate the timely on-boarding and off-boarding of user access;

(e) a dedicated system for generating, storing, and managing cryptographic keys used for encryption, decryption, and other cryptographic operations;

(f) a centralized system for managing identities and controlling access to resources;

(g) a centralized system for managing identities across multiple organizations or domains, allowing users to access resources and services without the need for separate user accounts in each domain (Identity Federation);

(h) a security posture management service to continuously monitor and assess the security controls and practices implemented to protect research data and systems;

(i) a centralized system for the management and administration of contracts signed between parties;

(j) a centralized system for systematically collecting, analyzing, and monitoring audit logs and activities across various systems, applications, and data repositories;

(k) a document version system for maintaining control, traceability, and collaboration when managing documents history, including comprehensive audit trails and the associated documentation;

(l) a centralized system to facilitate the secure and efficient exchange of data between various authorized parties, internal or external to the RE;

(m) dedicated workstation(s) or computing environment(s) that are specifically designed and configured to provide secure access to sensitive data;

(n) a process management system to enable repeatability and coordination of complex processes and workflows; and

(o) if applicable, a system to effectively manage, secure, and monitor the Application Programming Interfaces (API) that enable the exchange of data and services between systems and applications.

See Annex C for examples of baseline security controls.

4.8.9 The RE shall have documented procedures for ensuring that its capabilities listed under section 4.8.8 above are known to the relevant parties as required.

4.8.10 The RE shall have documented procedures for reviewing and updating the controls and capabilities described above, at minimum annually or more frequently if major changes occur (such as new controls or a vendor switch).

4.8.11 The RE shall have documented procedures for collaborating with Indigenous or non-Indigenous Communities to ensure that:

(a) practising secure data management does not overburden them, and

(b) access is provided to them for the resources required for their infrastructural needs.

4.8.12 The RE shall have documented procedures for describing the long-term disposition of research data, such as secure destruction, irreversible anonymization, archiving.

Informative Annexes

The following references were considered in the development of this NSC and may help the reader with the conceptual understanding.

Annex A: Informative References

Research Data Management in the Canadian Context: A Guide for Practitioners and Learners created by Kristi Thompson; Elizabeth Hill; Emily Carlisle-Johnston; Danielle Dennie; and Émilie Fortin published with Pressbooks. The original is freely available under the terms of the CC BY-NC 4.0 license at https://ecampusontario.pressbooks.pub/canadardm .

Annex B: Examples of Research Data Lifecycles (Informative)

Felicity Tayler; Marjorie Mitchell; Chantal Ripp; and Pascale Dangoisse, “Data Primer: Making Digital Humanities Research Data Public”, 2022, Annex 1, available online at: https://ecampusontario.pressbooks.pub/dataprimer/front-matter/annex-1-data-flow-and-discovery-model/, refers to the following elements: Consent, Data Collection, Data Processing, Critical Analysis, Sharing and Preservation.

US National Institutes of Health, National Library of Medicine, “Research Lifecycle”, available online at: https://www.nnlm.gov/guides/data-glossary/research-lifecycle, refers to the following elements of the research lifecycle: Plan, Acquire, Process, Analyze, Preserve, Share Results, and Reuse.

US Department of Commerce, National Institute of Standards and Technology (NIST), “Research Data Framework”, NIST SP 1500-18r2, version 2.0, available online at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/1500-18/NIST.SP.1500-18r2.html, refers to: Envision, Plan, Generate/Acquire, Process/Analyze, Share/Use/Reuse, Preserve/Discard

Winter, Caroline. "The Current State of Research Data Management in Canada: A Report by the Digital Research Alliance of Canada." Open Scholarship Policy Observatory, 3 Dec. 2021, https://ospolicyobservatory.uvic.ca/current-state-of-rdm/. refers to the following elements: Plan, Create, Process, Analyse, Disseminate, Preserve, Reuse

Annex C: Baseline Security Controls (Informative)

These controls are based on CIS Critical Security Controls Version 8. The controls listed in this document provide guidance on where/how controls should be applied at various levels from a RE perspective. Please reference the CIS controls version 8 document for more information about specific controls and their implementations.

Level 1 cybersecurity controls play a vital role in providing a solid baseline protection for REs, regardless of data sensitivity. These foundational controls are designed to establish essential security practices that, when implemented, create a robust defense against a wide range of cyber threats. By focusing on fundamental aspects, these controls set the stage for a strong security posture, creating a resilient foundation upon which more advanced security measures can be built. In an era of evolving cyber threats and increasing data breaches, adhering to level 1 cybersecurity controls is a proactive and prudent approach for REs to mitigate risks and ensure the confidentiality, integrity, and availability of their valuable research assets.

Level 2 cybersecurity controls take the protection of REs to the next level by offering enhanced security measures, particularly vital for organizations dealing with sensitive data. These controls encompass a more advanced set of practices and technologies to safeguard a diverse range of sensitive data types, such as personally identifiable information (PII), medical records, intellectual property, and classified research findings. For example, in the context of a healthcare RE, level 2 controls would include performing testing of the security controls as well as ensuring third-party service providers adhere to security requirements. These controls not only help prevent data breaches but also bolster the overall resilience of REs, ensuring they can meet stringent compliance requirements and maintain the trust of stakeholders, collaborators, and the individuals whose sensitive data they handle. In essence, level 2 cybersecurity controls are an essential investment in maintaining the integrity and security of critical research data.

Note: Application development cybersecurity controls are not in consideration for this standard. If the RE is also developing an application or application component to work with research data, consider the following controls:

- CIS Section 16
- OWASP ASVS

Adapted CIS Critical Security Controls for REs

CIS Number	Title/Description	Level 1	Level 2
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	X	X
1.2	Address Unauthorized Assets	X	X
1.3	Utilize an Active Discovery Tool		X
2.1	Establish and Maintain a Software Inventory	X	X
2.2	Ensure Authorized Software is Currently Supported	X	X
2.3	Address Unauthorized Software	X	X
2.4	Utilized Automated Software Inventory Tools		X
2.5	Allowlist Authorized Software		X
2.6	Allowlist Authorized Libraries		X
3.1	Establish and Maintain a Data Management Process	X	X
3.2	Establish and Maintain a Data Inventory	X	X
3.3	Configure Data Access Control Lists	X	X
3.4	Enforce Data Retention	X	X
3.5	Securely Dispose of Data	X	X
3.6	Encrypt Data on End-User Devices	X	X
3.7	Establish And Maintain a Data Classification Scheme	X	X
3.8	Document Data Flow	X	X
3.9	Encrypt Data on Removable Media	X	X
3.10	Encrypt Sensitive Data in Transit	X	X
3.11	Encrypt Sensitive Data at rest	X	X
3.12	Segment Data Processing and Storage Based on Sensitivity		X
3.13	Deploy a Data Loss Prevention Solution		X
3.14	Log Sensitive Data Access	X	X
4.1	Establish and Maintain a Secure Configuration Process	X	X
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	X	X
4.3	Configure Automatic Session Locking on Enterprise Assets	X	X
4.4	Implement and Manage a Firewall on Servers	X	X
4.5	Implement and Manage a Firewall on end-user devices	X	X

CIS Number	Title/Description	Level 1	Level 2
4.6	Securely Manage Enterprise Assets and Software	X	X
4.7	Manage Default Accounts on Enterprise Assets and Software	X	X
4.8	Uninstall or Disable unnecessary services on enterprise assets	X	X
4.9	Configure Trusted DNS Servers on Enterprise Assets		X
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		X
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		X
5.1	Establish and Maintain an Inventory of Accounts	X	X
5.2	Use Unique Passwords	X	X
5.3	Disable Dormant Accounts	X	X
5.6	Centralize Account Management	X	X
5.7 (new)	Configure step-up, adaptive, or just-in-time authentication for administrative functions		X
6.1	Establish an Access Granting Process	X	X
6.2	Establish an Access Revoking Process	X	X
6.3	Require MFA for Externally-Exposed Application	X	X
6.4	Require MFA for Remote Network Access	X	X
6.5	Require MFA for Administrative Access	X	X
6.7	Centralize Access Control	X	X
6.8	Define and Maintain Role-Based Access Control	X	X
7.1	Establish and Maintain a Vulnerability Management Process		X
7.2	Establish and Maintain a Remediation Process		X
7.3	Perform Automated Operating System Patch Management	X	X
7.4	Perform Automated Application Patch Management	X	X
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		X
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		X
7.7	Remediate Detected Vulnerabilities		X
8.1	Establish and Maintain an Audit Log Management Process	X	X
8.2	Collect Audit Logs	X	X
8.3	Ensure Adequate Audit Log Storage	X	X

CIS Number	Title/Description	Level 1	Level 2
8.4	Collect Detailed Audit Logs	X	X
8.9	Centralize Audit Logs		X
8.10	Retain Audit Logs		X
8.11	Conduct Audit Log reviews		X
8.12	Collect Service Provider Logs		X
9.1	Ensure use of only fully supported browsers and email clients	X	X
9.2	Use DNS Filtering Services		X
9.3	Maintain and Enforce Network-Based URL Filters		X
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		X
9.5	Implement DMARC		X
9.6	Block Unnecessary File Types	X	X
9.7	Deploy and Maintain Email Server Anti-Malware Protections	X	X
10.1	Deploy and Maintain Anti-Malware Software	X	X
10.2	Configure Automatic Anti-Malware Signature Updates	X	X
10.3	Disable Autorun and Autoplay for removable media	X	X
10.4	Configure Automatic Anti-Malware Scanning of removable media		X
10.5	Enable Anti-Exploitation Feature		X
10.6	Centrally Manage Anti-Malware Software		X
10.7	Use Behavior-Based Anti-Malware Software		X
11.1	Establish and Maintain a Data Recovery Process	X	X
11.2	Perform Automated Backups	X	X
11.3	Protect Recovery Data	X	X
11.4	Establish and Maintain Isolated Instance of Recovery Data		X
11.5	Test Data Recovery		X
12.1	Ensure Network Infrastructure is up-to-date	X	X
12.2	Establish and Maintain a Secure Network Architecture		X
12.3	Securely Manage Network Infrastructure		X
12.4	Establish and Maintain Architecture Diagrams		X
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		X

CIS Number	Title/Description	Level 1	Level 2
12.6	Use of Secure Network Management and Communication Protocols		X
13.1	Centralized Security Event Alerting		X
13.2	Deploy a Host-Based Intrusion Detection Solution		X
13.3	Deploy a Network Intrusion Detection Solution		X
13.4	Perform Traffic Filtering between network segments		X
13.5	Manage Access Control for Remote Assets		X
13.6	Collect Network Traffic Flow Logs		X
13.10	Perform Application Layer Filtering		X
14.1	Establish and Maintain a Security Awareness Program	X	X
14.2	Train Workforce members to recognize social engineering attacks	X	X
14.3	Train workforce members on authentication best practices	X	X
14.4	Train workforce on data handling best practices	X	X
14.5	Train workforce members on causes of unintentional data exposure	X	X
14.6	Train workforce members on recognizing and reporting security incidents	X	X
14.7	Train workforce on how to identify and report if their enterprise assets are missing security updates	X	X
14.8	Train workforce on the dangers of connecting to and transmitting enterprise data over insecure network	X	X
14.9	Conduct Role-Specific Security Awareness and Skills Training		X
15.1	Establish and maintain an inventory of service providers	X	X
15.2	Establish and maintain a service provider management policy		X
15.3	Classify Service Providers		X
15.4	Ensure service provider contracts include security requirements		X
16.4	Establish and Manage an Inventory of Third-Party Software Components	X	X
16.5	Use Up-to-date and Trusted Third-party software components	X	X
17.1	Designate Personnel to manage incident handling	X	X
17.2	Establish and maintain contact information for reporting security incidents	X	X
17.3	Establish and maintain an enterprise process for reporting incidents	X	X

CIS Number	Title/Description	Level 1	Level 2
17.4	Establish and maintain an incident response process	X	X
17.5	Assign Key Roles and Responsibilities		X
17.6	Define Mechanisms for communicating during incident response		X
17.7	Conduct routine incident response exercises		X
17.8	Conduct Post-Incident Reviews		X
18.1	Establish and Maintain a Penetration Testing Program		X
18.2	Perform periodic external penetration tests		X
18.3	Remediate Penetration Test Findings		X
18.4	Validate Security Measures		X
18.5	Perform Periodic Internal Penetration Tests		X