Dialogue

Information Security Policy is here:

https://www.notion.so/godialogue/Dialogue-Information-Security-Policy-afa358fd24764f8ab3510c7d59c3c9e4?pvs=4

Version 6.0 (29-Mar-2024)

Approved by Alexis Smirnov, CTO

Table of contents

0 - Introduction

Dialogue collects, processes, stores and transmits information in many forms. It is vital that Dialogue protects this information against both deliberate and accidental threats and vulnerabilities.

ISO/IEC 27002 is a widely-recognized international standard that helps organizations secure both their own information assets and those of their customers. Dialogue follows ISO 27002 for its Information Security Policy.

Dialogue's information assets can be subject to both deliberate and accidental threats. Because processes, systems, networks and people have inherent vulnerabilities, information security risks are always present. Effective information security reduces these risks by protecting Dialogue against threats and vulnerabilities, and then reduces impacts to its assets.

Dialogue achieves information security by implementing a set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. This Information Security Policy is the foundation of Dialogue's set of controls that mitigate information security risks.

However, successful management of Dialogues information security requires support from all employees and contractors, as well as from our shareholders, suppliers and other external parties. That support assures all stakeholders that Dialogue's assets are reasonably safe and protected against harm.

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. Similarly, information systems have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage, and changes to existing systems present Dialogue with opportunities to update and improve security controls.

1 - Scope

This policy gives guidelines for organizational information security standards and management practices that take into consideration Dialogue's individual information security risk environment. The policy is designed to support SOC2 information security controls and guidelines and is based on both ISO/IEC 27002:2013 and commonly accepted information security controls.

2 - Normative References

The normative reference for this Information Security Policy is the ISO/IEC 27002:2013 document "Information technology: Security techniques and Code of practice for information security controls".

3 - Terms and Definitions

In this policy, unless the context otherwise requires:

"**Agent Personnel"** means all employees, agents, consultants and contractors of the Dialogue and/or of any Sub-contractor;

"**Contractor**" means any third party from time to time providing goods or services (or goods and services) to Dialogue in connection with the performance of the Services;

"Dialogue Compliance Manager" means the person appointed to that role by Dialogue.

"Dialogue Security Director" means the person appointed to that role by Dialogue

"Dialogue Systems" means the information technology systems and networks including all applications, databases, operating systems, hardware and software owned by, or licensed to, Dialogue which is used by or on behalf of Dialogue in the provision of the Services;

"**Data"** means all data, information, text, images, drawings and other materials which are embodied in any medium including all electronic, optical, magnetic or tangible medium and which are supplied to Dialogue by a user or which Dialogue is required to generate, collect, process, store or transmit in connection with this Security Policy;

"**Good Industry Practice**" means the exercise of reasonable skill, care, prudence, efficiency, foresight and timeliness which would be expected from a reasonably and suitably skilled, trained and experienced person;

"**Incident"** means any event having an adverse impact on Dialogue's ability to provide the Services, Client's ability to receive the Services or that otherwise has an adverse impact on Dialogue's ability to perform its obligations under this Schedule;

“**Incident Management Process**" means Dialogue’s process for the effective management of incidents to ensure minimum detriment to and continued provision of the Services in compliance with Dialogue’s obligations under this Policy;

“**Information Security Architecture”** means the methodology, design, tools, processes and systems used by Dialogue for the purpose of ensuring the security of information at every point in Dialogue Systems in accordance with the Information Security Policy and in order to provide the Services in compliance with Dialogue’s obligations under this Security Schedule;

“**Information Security Policy**" (this document) means a document that states Dialogue’s strategy, direction and commitment for information security, setting out its approach to managing information security to ensure an appropriate set of security controls are defined, documented and implemented across Dialogue’s business in accordance with business requirements and relevant laws and regulations and forming the basis of Dialogue’s standards, policies, procedures and practices;

“**ITSM Ticketing System**” means the IT Service Management tool used to log incidents, service request and perform change management

“**IP**” means Intellectual Property;

“**Malicious Code**" means any software, virus, Trojan horse, time bomb or other code (which can take the form of but not be limited to Java applets, scripting languages, browser plug-ins or pushed content) that is harmful, disabling or which enables unauthorized access to or theft of or damage to Data or other information or otherwise impairs the operation of Dialogue Systems.

“**Material Adverse Effect**" means an adverse effect or impact on the Services, Dialogue’s ability to provide the Services or otherwise perform its obligations under this Security Policy, user's ability to receive the Services or has the potential for the foregoing to occur, and shall include situations where:

- Dialogue reasonably believes that loss or damage to Data be greater than thirty thousand Canadian dollars ($30,000 CAD);
- Dialogue reasonably believes that there is a real risk of significant harm or injury that can be caused to users or clients;
- adverse media interest to Dialogue clients, in Dialogue’s reasonable opinion, is likely to be generated;
- there has been a material failure in, or to comply with, Dialogue’s security guidelines and procedures; or
- Dialogue reasonably believes that Dialogue clients would desire to be informed;

“**Payment Card Industry Data Protection Standards**" means the payment card industry data protection standards as published from time to time by the Security Standards Council;

“**PHI**” means Personal Health Information

“**PII**” means Personally Identifiable Information

“**Privileged User Access”** means access to a system where the user has permission and rights beyond those of normal users; for example, Windows Administrators, Unix Root Accounts or derivatives thereof;

“Security Assessment (pentesting and/or vulnerability scanning)” means tests performed on Dialogue Systems in order to:

a) identify design and/or functionality issues in applications or infrastructure;

b) probe for weaknesses in applications, network perimeters or other infrastructure elements, as well as weaknesses in processes or technical countermeasures;

c) identify potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws including, **but not limited to**, the following examples for infrastructure and application testing;

i. invalidated or unsanitized input;
ii. insufficient access control controls;
iii. weak authentication and session management;
iv. cross-site scripting (XSS) flaws;
v. remote code execution;
vi. memory corruption (i.e. buffer / stack overflow, out-of-bounds reads, pointer arithmetics);
vii. injection flaws (SQL, LDAP, etc.);
viii. improper error handling;
ix. insecure storage (no data protection / encryption);
x. denial of service;
xi. insecure configuration management;
xii. proper use of TLS;
xiii. proper use of encryption; and
xiv. antivirus reliability and testing, which could expose Dialogue to risks from malicious activities.

Such assessment will typically incorporate activities also commonly referred to as penetration testing.

“Security Assessment Vendor” means a suitably qualified third party employed to perform an independent *Security Assessment*.

“**Significant Attack**" means an action with intent to cause harm to Dialogue Systems or Client Systems, including any form of unauthorized access to a system or action resulting in any degradation of a system. To clarify, this would be more than scanning for vulnerabilities in systems through, for example, scanning a range of IP addresses;

“**Security Incident**" means an event (or chain of events) that compromises the confidentiality, integrity or availability of Data or Dialogue Systems, or violates Dialogue’s information security policies or standards or the requirements of this Security Policy;

“**Services**” means all services provided to Dialogue clients by Dialogue when acting pursuant to and in accordance with this Security Policy.

Update log

Version #	Date	Document change history
v1.1	05-Jun-2018	Updated client notification timeline in case of a Security Incident.
v1.2	12-Oct-2018	Updated following the review by MedOps.
v2.0	Mar-2020	Periodic review and update
v3.0	Mar-2021	Periodic review and update. Addition of Information Security Director role. Improve logging and monitoring section, Incident Response section and add anonymous feedback policy.
v4.0	Mar-2022	Periodic review and update. Addition of ITSM ticketing system. Addition of CloudFlare. Updated password requirements. Update to secure areas. Changes to Incident Management. Changes to remote work policy.
v5.0	Mar-2023	Periodic review and update. Update to Information security roles and responsibilities. Update to Mobile device policy. Update to Information security awareness, education and training. Update to Terminations and change of employment. Update to acceptable use of assets. Update to access control policy. Update to Management of privileged access rights. Update to Management of secret authentication information of users. Update to Access control to program source code. Update to Protection from malware. Update to Backup. Update to Logging and monitoring. Update to Control of operational software. Update to Technical vulnerability management. Update to Information security in supplier relationships. Update to Incident reporting procedure.
v6.0	Mar-2024	Periodic review and update Update to Review of the policy for information security Update to Information Security roles and responsibilities

		Update to Contact with authorities Update to Contact with special interest group Update to Mobile device policy Addition of subsection 6.2.3 Clean desk policy Update to Acceptable use of assets Addition of subsection 8.1.3.a Follow all applicable laws Update to Protection of malware Addition of subsections to Control of operational software - 12.5.1Installation of software onto the cloud environments includes deployment procedures - 12.5.2 Installation and download of software on company owned End-User devices Update to Information Security in supplier relationship Update to Summary of responsibilities and procedures Update to Independent review of information security Update to Compliance with the security policy

4 - Structure of this document

4.1 Clauses

In this Information Security Policy, each clause defining security controls contains one or more main security categories. The order of the clauses in this document does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important. Furthermore, lists in this standard are not in priority order.

4.2 Control categories

Each main security control category contains:
a) a control objective stating what is to be achieved;
b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control
Defines the specific control statement, to satisfy the control objective.

Implementation guidance
Provides more detailed information to support the implementation of the control and meeting the

control objective. The guidance may not be entirely suitable or sufficient in all situations, and may not fulfill the organization's specific control requirements.

Other information
Provides further information that may need to be considered, for example legal considerations and references to other standards. If there is no other information to be provided, this part is not shown.

5 - Information security policies

Information security and its control environment at Dialogue is one of the pillars of its activities. It sets the tone of the organization and influences the awareness of its personnel. The policy sets the operating environment that includes strong values shared by the entire team. Other components of this environment include management's commitment to excellence; Dialogue's organizational structure; the processes of assignment of authority and responsibility; Dialogue Privacy Policies (for patients and for employees and contractors); the oversight and direction provided by the Executive Management, the Senior Executive Management and the Board of Directors, a risk management process with a mitigation plan, dissemination of relevant information through various methods of communication, and monitoring to evaluate the effectiveness of controls and their enhancement.

The primary objective of this policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1 - Management direction for information security

(CC1.2, CC2.1)

5.1.1 Policies for information security
Adherence to the information security policies defined in this document addresses the following requirements:

- Dialogue must be a trusted service provider to its customers.
- Dialogue must earn and maintain the highest degree of trust from its users.
- Dialogue must abide by all applicable regulations that govern the delivery of healthcare services in Canadian provinces and territories where Dialogue operates. More specifically, this implies that Dialogue must secure the healthcare records of the patients using its service.
- Dialogue must respect legal requirements set forth in contracts with its clients, distribution partners and medical professionals.
- Dialogue operates in the challenging security environment of the public Internet, where it must provide access to quality care through consumer devices such as mobile phones and personal computers owned and operated by its patients.

5.1.2 Review of the policies for information security

The policies for information security are reviewed yearly, every first quarter of each fiscal year, or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. In case of an update, notices are sent to all employees and contractors after the update is complete.

The reviews include assessing opportunities for improvement of the organization's policies and approach to management of information security in response to changes to its organizational environment, business circumstances, contractual requirements, regulatory compliance, emergent threats or technical environment.

The reviews also include risk assessment of Dialogue operations. During the risk assessment, risks are rated using a risk evaluation process and ratings based on the impact and the probability that a risk occurs, and are mitigated through a specific action plan. (CC3.1, CC3.3, CC4.1)

The overall ownership and accountability for this policy is with the Chief Information Security Officer (CISO)). This policy is reviewed annually by the Executive Management Team (EMT). The policy statements take the reviews into account. All updates to the policy are approved by the CTO.

5.1.3 Policy exception process

Unless otherwise explicitly defined in a specific section of this policy document, it is expected by the executive team that all employees and contractors of the organization comply fully with all policies contained in this document. However, there may be cases where compliance cannot be achieved for various reasons. In such cases, an exception must be documented and approved using the following process.

5.1.3.1 Acceptable exception scenarios

The following scenarios may be considered for an exception to a documented Information Security policy:

- *Temporary* exception, where immediate compliance would disrupt critical operations
    - A rare and time-limited occurrence. Repeated occurrence shall be further investigated.
- Another acceptable solution with equivalent protection is available
    - In which case, the alternate solution may be considered for a further revision of the policy.
- Applicable to a legacy system scheduled for deprecation where immediate compliance is not technically achievable
    - Risk management process is applied and considers the amount of time during which the legacy system will remain in operation.
- Long-term exception, where compliance would severely impact the business
    - A rare occurrence. Changes to the policy must be considered for a further revision of the policy document to remove the exception within 90 days.

- Compliance would have major financial impact that would not be offset by the reduction of risk brought by compliance (i.e. compliance cost offsets the risk of non-compliance)
    - Balancing compliance *vs* non-compliance may have ethical and legal implications. If so, they are considered, evaluated and documented by the Executive Management team. If required, the policy is updated.

5.1.3.2 Documenting an exception request

Every exception request must include the following information elements:

- The policy for which an exception is being requested
- The device, application or service for which an exception is being requested
- The type of data that will be affected, either directly or indirectly, by the exception
- The nature of the non-compliance (description of how it differs from the policy)
- The reason for requesting an exception is required (e.g.. Business need or particular scenario as well as alternatives that have been considered)
- Assessment of the potential risk posed by non-compliance (i.e. if exception is granted)
- Plan for mitigating possible risks (i.e. compensating controls, alternative methods)
- Expected time period for non-compliance

5.1.3.3 Exception granting process

1. The requester must submit the request, via the ITSM ticketing system, containing the information elements described in the previous section to the Information Security Director.
2. The Information Security and Compliance functions will evaluate if the exception corresponds to one of the acceptable scenarios, analyze the elements provided and perform, as needed, additional risk assessment activities before deciding whether to:
    a. Deny the exception request
    b. Grant a Temporary exception with an expiration date
    c. Grant a Long-Term exception
3. The Information Security Director will give the decision to the requester and keep a record of the request and the decision. The record shall be stored in the ITSM ticketing system with restricted access control to prevent tampering of the logbook by other employees. The CTO, Information Security and Compliance functions shall all have visibility into this document so that they are aware of deviations.

5.1.4 Guiding principles

The following principles guide all activities relating to information security.

- Security, privacy and trust are key business requirements to consider when making decisions.
- Security considerations should account for the rapidly evolving nature of the organization's technology, its products, and services as well as external threats.
- Security controls must be balanced with the priorities of a rapidly changing and fast growing business.

6 - Organization of information security

The objective of this Information Security Policy is to establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1 Internal organization

6.1.1 Information security roles and responsibilities

(CC7.1)
Dialogue's CEO manages Dialogue's activities daily with the assistance from a Senior Executive Management team representing all functions of the business. Members of the SEMT draw experience from their former roles as leaders of organizations specializing in software, sales, customer services, consultancy, and healthcare and enterprise services.

In his role, the CEO assigns authority and responsibility for operating activities, and establishes reporting relationships and authorization hierarchies. The SEMT designs policies and communications so that personnel understand Dialogue's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Lines of authority and responsibility are clearly established throughout the organization under the CEO. These lines of authority and the associated responsibilities are communicated through: (1) Shared corporate values (2) organizational structure, (3) commitment to competence and accountability, and (4) policies and procedures. Managers are expected to be aware of their responsibilities and lead employees in complying with Dialogue's policies and procedures.

The CTO is responsible for the development, maintenance and operation of Dialogue Systems (see section 14). In this role, the CTO assigns the authority and responsibility for associated functions, processes and policies. The CTO has overall responsibility for the information security. The Information Security function is led by the Chief Information Security Officer with assistance from the Information Technology Director & Director of Platform Engineering.

One or several roles may be assigned to individuals. Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless, they remain accountable and should determine that any delegated tasks have been correctly performed.

The following roles within Dialogue are related to information security:

- The CTO reviews and approves the information security policy, and informs the CEO of changes.
- The Chief Privacy Officer provides input on privacy issues based on the evolving privacy landscape and on incidents or vulnerabilities that require investigation.
- System Administrator performs overall system administration and changes of the system

- Software Developer is responsible for implementing security requirements within software
- The Security Architect responsibilities are shared by the Chief Information Security Officer, Director of Platform Engineering and the Director of IT & Security (all under the CTO). Responsibilities include defining Information Security (IS) requirements and assuring that the system design meets security requirements.
- The Product Manager is responsible for integrating IS requirements in product specifications.
- The Engineering Team Lead is responsible for ensuring the product implementation meets the quality level specified in product requirements, including IS requirements.
- Service Ops (Medical Operations) Staff regularly handle patient's Personal Health Information
- Compliance Manager documents policies and procedures, assures adherence, identifies non-compliant events and works with stakeholders to remediate such events.

Roles with access to assets include specific responsibilities as defined by sections 8.1.1 and 8.1.2

Vetting and qualification review is performed during the recruitment process through a series of focused interviews and case studies. Whenever an individual is assigned to a new role within the information security function, the CTO (in consultation with CISO) approves the appointment, considering the individual's demonstrated qualifications. The qualification review also applies to suppliers (contractors, consultants) (ref. ISO 27001:2013 6.1.1.d, 6.1.1.e)

An organizational chart is in place to communicate the defined key areas of authority, responsibility and lines of reporting to personnel related to the design, development, implementation, operation, maintenance and monitoring of the system. (CC1.1, CC1.2)

All components of Dialogue Systems have an owner who is ultimately responsible for ensuring security of the asset, and a designated individual who should be informed of all security measures of the asset. When the owner has to delegate access or control, he must ensure that the people have been sufficiently trained and are aware of their responsibilities.

6.1.2 Segregation of duties
(CC5.1)
It should be recognized that Dialogue is a small and nimble organization and as such formal segregation of duty is currently difficult to achieve. Nevertheless, the principle should generally be applied as far as possible and practicable. There should never be an individual with access to every production system at once; checks and balances shall be in place. One or several roles may be assigned to individuals. Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless, they remain accountable and should determine that any delegated tasks have been correctly performed.

The number of people with administrative access to production systems is strictly minimized.

As a compensating control for the lack of segregation of duties, all critical systems (AWS, Auth0, GitHub, etc.) have a non tamperable audit trail that shall be reviewed quarterly to detect anomalous usage.

6.1.3 Contact with authorities

(CC3.3)
In the event of a major incident, the response cell leader is responsible to escalate it to the SEMT. The SEMT is responsible to determine which authorities must be contacted. The Chief Information Security Officer is responsible for contacting the authorities along with other members of the SEMT, privacy, compliance and legal teams, as appropriate. Also see section 16.

A list of the government agencies or contact persons shall be maintained by the Compliance Manager or delegate.

6.1.4 Contact with special interest groups

(CC3.3)

Dialogue is tracking the developments in the following areas:

- AWS and Cloudflare Cloud Security
- Okta, SentinelOne, and Google Cloud Security
- Healthcare
- Privacy of healthcare records
- Web application development
- Mobile application development

In addition, Dialogue consults with Sun Life CyberSecurity function and other special interest groups facing similar concerns

- AEHIS (Association for Executives in Healthcare Information Security)
    - https://aehis.org/
- Guide to InfoSec for the Healthcare Sector (Ontario Government)
    - https://ehealthontario.on.ca/en/security/guides
- Healthcare InfoSec resources
    - https://www.healthcareinfosecurity.com/resources
- HIMSS (Healthcare Information and Management Systems Society)
    - https://www.himss.org/resources-all
- H-ISAC (Health Information Sharing and Analysis Center)
    - https://h-isac.org/
- Digital Health Canada
    - https://digitalhealthcanada.com/

6.2 - Mobile devices and teleworking

(CC5.7, CC5.8)
This policy is designed to ensure that information security is considered and enforced in the teleworking personnel work environment. This is especially relevant for our health care professionals (HCP) as the majority of them work outside the organization's headquarters. The following section also defines guidelines with regard to the use of mobile devices that access business information such as e-mail or other collaboration software.

6.2.1 - Mobile device policy

This policy is designed to manage risks introduced by the use of mobile devices. Mobile devices include, but are not limited to:

- Laptop computers
- Mobile phones (smartphones)
- Chromebooks, tablets

More generally, this policy should cover any device that has the capability of storing sensitive corporate information (IP, PII, PHI etc. - as defined in section 8.1.1) and that can be carried easily and/or regularly outside the premises of the organization where they may not benefit from the same degree of physical security and oversight as if they were permanently installed in the organization's office. As such, it is important to recognize that it is not so much about the specific type of device, but that their small form factor makes it easy for them to be stolen, lost or temporarily captured by an unauthorized person that could compromise them (i.e. “evil maid attack”) before returning them where they were found. Technology evolves quickly, and it’s easy to think that new types of devices (such as wearables, etc.) could meet the criteria to be covered by this policy.

All device types listed here can be grouped in two categories: company-owned or employee-owned (BYOD - Bring Your Own Device). Those categories may have an impact on the level of policy enforcement, as well as the type of data that is authorized to be stored on them.

Full time employees use company-owned laptops. An inventory registry is maintained and updated during onboard, offboard, and purchases and includes serial number and/or other unique identifiers.

Employees must declare theft or loss as soon as possible to their manager and to the Dialogue Information Technology team. In this case, System Administrators are responsible for revoking access to associated accounts, remote wiping the device, and rotating credentials.

Employees must maintain the configuration of all hardware devices used for work-related purpose (Dialogue-owned or personal) to assure that all the security controls are in place, such as:

- Full Disk encryption
- “Strong” device password (as defined in section 13.1)

- Device lock after a period of inactivity
- Antivirus (as defined in 12.2)
- Operating System firewall enabled
- Automated OS and application updates

Access from mobile phones to work-related data using tools (such as Slack, Gmail, UKG) can be restricted or blocked if the mobile device does not have a company approved device policy app (MDM Mobile Device Management agent) installed. The MDM agent allows Dialogue to enforce strong security controls such as device encryption, blocking compromised devices and remote device wiping.

Sensitive or confidential data should not be stored locally on mobile devices unless it is necessary for business operations and approved by the IT team. When stored, this data must be encrypted using robust encryption algorithms to prevent unauthorized disclosure. The utilization of file-sharing services on mobile devices is strictly forbidden to ensure data integrity, compliance with industry regulations, and protection of PHI and PII.

6.2.2 - Teleworking

Teleworking occurs when an employee, a contractor actively working on Dialogue work, or more often healthcare professionals perform work on behalf of Dialogue outside the headquarters.

Teleworking is allowed under specific conditions:

- Teleworking is allowed across all functions, while employees are encouraged to work from our offices, when the opportunities occur, or when some of them need to respond to a business need (e.g. on-site presence required, due to the nature of a role).
- The majority of healthcare professionals work from their own office, so they are teleworkers by default
    - There is a contractual agreement which defines requirements for performing medical work outside the headquarters.
    - Refer to the appropriate sections of the contractual agreement, entitled “Technical Specifications and Data Policy”.

6.2.3Clean Desk Policy

In order to maintain a secured workspace all users will do the following:

• All protected data, electronic or paper, must be secured in their work area at all times.

• All devices must be locked when the workspace or device is unoccupied.

• Workstations must be shut down completely at the end of the workday.

• Laptops must be secured at the end of the day by shutting down and locking in a secured location or being put to sleep and kept with the employee in a secure location.

• Any protected information must be removed from the desk and locked in a drawer when the work area is unoccupied or at the end of the day.

• Keys used to access protected information must be secured at all times. They must not be left unattended at any time.

• Passwords must never be written down. For example, no passwords should be on sticky notes in an employee's work area, including under keyboards or attached to monitors.
• All documents containing protected data, that are printed or used to make photocopies, must be removed from printers, copiers or multifunction devices as soon as possible. Avoid printing this information if it can not be removed immediately.
• Whiteboards containing protected data must always be erased at the end of the day. They should be documented if the information is needed and secured accordingly.
• At the end of the day, each desk is inspected by the employee to ensure it follows the Clean Desk Policy.
• File cabinets containing protected data must be kept closed and locked when they are not being actively used.
• Documents or electronic media containing protected data must never leave the office or workspace without approval from management or the Security Team.
• All personal items must be stored under the desk or in a secured area. They should not be left unattended at any time.

7 - Human resources security

7.1 - Prior to employment

7.1.1 Screening
New employee and contractor hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.

Each employee and contractor must pass a set of interviews, reference checks, and a background check done by a 3rd party service. Records of each step are kept by the HR department. (CC1.3, CC1.4)

7.1.2 Terms and conditions of employment
Employees and contractors must sign both a standard contract and a confidentiality agreement that outline their responsibilities regarding Information Security and that refer to the current document.

7.2 - During employment

Employees and contractors with responsibility for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, must have information necessary to carry out those responsibilities. Policy and procedures documents for significant processes are available on the intranet (Ultipro, Google Drive, Notion). (CC2.4)

The employees and contractors must accept the Code of Conduct and Confidentiality Agreement at onboarding and reaffirm their agreement annually. Compliance with those activities is tracked and reported to EMT annually. (CC1.4, CC2.2, CC2.3)

Formal job descriptions exist for all active and approved positions and are defined during the hiring process. These documented position descriptions are in place to define the skills, responsibilities and knowledge levels required for particular jobs. (CC1.1, CC1.2, CC1.3)

The Team Manager performs an individual performance review of all team members to ensure employees have all the necessary feedback about their level of performance in their responsibilities and that the individual is in the right place within the organizational structure. (CC1.1)

7.2.1 Information security awareness, education and training

All employees and contractors of Dialogue receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Onboarding process is tailored to job functions. Onboarding training and education materials include aspects of information security appropriate to the position. Specifically:

- All employees must read, agree and abide by the formal confidentiality agreement.
- Software Engineering onboarding includes awareness of secure coding best practices and standards
- Care Team's onboarding includes training on tools and processes of handling PHI
- Sales and Customer Success teams receive training on proper handling of financial information

(CC1.3, CC1.4, CC2.2)
Training policy is in place for employees to maintain and advance the skill level of personnel.

(CC1.3)
All employees and contractors must complete Dialogue's standard training on information security awareness at onboarding and at least annually thereafter. Management uses an information security training platform to create and validate a completion report that documents that all employees and contractors fulfill their obligations. (CC1.3) Failure to complete mandatory security training could result in disciplinary actions.

7.3 - Termination and change of employment

(CC5.2, CC5.4)
Termination follows a standard HR process and includes a written notice to the employee (termination letter).

The employee's direct manager and IT team is responsible for the completion of the offboarding checklist. IT tracks the offboarding tasks (device retrieval and user deactivation) via a Jira ticket initiated from an official request by HR.

A change of role is recorded in the HR tracking system (Ultipro) and triggers the review of the access permissions. Employee or contractor user IDs are removed as of the date of employment based on changes in the human resource management system. Data assets under the employee's or contractor's account (emails, documents) are transferred to their direct supervisor.

Terminated contractors' and employees' ID may be re-routed to someone else in the same team to ensure external communications mechanisms are retained, or renamed with an alias to retain access by other members of the team, while ensuring that the terminated employee or contractor can no longer have access to it.

The access is removed or updated with accordance to section 9.2.4

8 - Asset management

8.1 - Responsibility for assets

(CC3.1)

8.1.1 Inventory

- Company-owned electronic devices
    - Laptops and computers
    - Mobile test devices
    - Networking equipment
- Authentication / credentials
    - Secret authentication material (SSH keys, IAM, OAuth tokens, hardware keys, etc.)
- IP (Intellectual property)
    - Business plans, strategy, processes, legal documents, etc.
    - Source Code of the application
    - ML models
- PII (Personally Identifiable Information)
    - Basic patient records (name, contact information, etc.)
    - Employee records
- PHI (Personal Health Information)
    - When health information is linked directly or indirectly to PII
- De-identified health information
    - For service improvement / quality control, etc.

8.1.2 Ownership of assets

Ownership of different types of assets is assigned by roles as defined in section 6.1.1

- Most employees and contractors
    - They are responsible for protecting access to the laptop they are assigned and keeping it updated by respecting the policy on mobile devices.
- Service Ops staff
    - They are responsible for using patient records (PHI) in an ethical and privacy-protective manner as necessary for providing care to patients, and for not copying data outside the Care Platform except during transfer to the Electronic Medical Record. Likewise, they are expected to log out of the CP as soon as they are done with their work session.
- System Administrator
    - They are responsible for protecting access to secret Authentication material for privileged access to systems they are assigned to manage.

- Software Developer
    - They are responsible for protecting access and integrity of the source code they develop.
- Security Architect
    - They are responsible for internal architectural documents.
- Product Manager
    - They are responsible for protecting access to strategy, road map documents.
- Engineering Team Lead
    - They are responsible for protecting access to mobile test devices used for QA purposes, as well as validating that the platform is behaving as designed for protecting access to critical information like PII and PHI.

8.1.3 Acceptable use of assets
Dialogue-owned assets provided to employees should be used solely for their intended work purpose and not for any personal work or activities not related to company employment. Non-work related files and documentation on company-issued devices are subject to deletion and will not be recovered in case of loss or employee offboarding.

Regarding data classified as “Restricted PHI” (as defined in section 8.2), it shall only be used to provide care to patients, shall never be used outside that context, and shall not be accessed from outside of Canada.

8.1.3.a Follow All Applicable Laws
Follow copyright, trade secret, patent, or other intellectual property laws, as well as similar laws or regulations. Without permission from the rights holder, violations could include:
• Installing or distributing pirated or other unlicensed software.
• Copying copyrighted material.
• Distributing copyrighted material.
• Never actively obtain or share material that violates sexual harassment or hostile workplace laws.

8.1.4 Return of assets
Regarding data classified as “Restricted PHI”, the method for “returning” those assets is achieved by disposing of media in accordance with section 8.3.2 and by logging out of the Care Platform, which will prevent further access and assure that data is not retained on any local storage.

8.1.5 Clarification regarding Credit Card information
No Credit Card information is accessed by Dialogue employees or contractors. No such information is stored on Dialogue systems. PCI-compliant systems are used to store credit card information and process payments. As such, Dialogue declares its systems as out of scope for PCI-DSS 3.0, as per the Self-Assessment Questionnaire A for “fully outsourced” scenarios.

8.2 - Information classification

(CC5.7)
This section presents the organization's different classifications that can be applied to documents, data and any other information, either in digital format or otherwise.

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Levels	Usage description	Examples
Public	Information that may be distributed to any entity outside the organization without any further acceptance process.	● Marketing information about actively distributed products and services ● End-user documentation ● Approved contributions to Open Source projects ● Standard price lists for small clients
Confidential	Information that may only be used by active employees or relevant contractors who have signed a confidentiality agreement while adhering to all data protection methods (as defined in this document). When there is a specific business need for some piece of information to be shared with other entities (ex. contractors, clients, etc.), the distribution must be approved by the executive team and legally protected under a Non Disclosure Agreement. Moreover, such information should be shared using authorized methods for which Authentication, Authorization and Auditing, as well as data at rest and in transit encryption can be assured.	● Source code ● Unannounced products and services ● List of customers ● Client's contact information ● NPS comments ● Internal price lists for larger clients ● Business processes ● Anonymized health information
Restricted secret	In addition to abiding to all rules applicable to the Confidential classification, information of this level shall always only be accessed or shared with strict adherence to the principles of The Least Privilege and made available to employees and contractors of Dialogue on a Need-to-know basis.	● Customer data ● Employee records ● Credentials to production systems ● Key material used to protect data rest or in transit for production systems ● Member PII
Restricted PHI	In addition to abiding to all rules applicable to "Restricted Secret" data, this type of data shall only be accessed by Service Ops staff and licensed medical professionals, who have valid reason to access the record, in relationship with medical care of a given patient.	● When linked to member PII (name, identifiers of any kind, etc.) ○ Health condition ○ Health history ○ Consultation history

	In addition, privileged access by system administrators may occur in the normal course of system maintenance or troubleshooting, but this kind of access should be exceptional and disinterested (not interested in a given patient record).	○ Care plan for the individual ○ Individual's health number

Threats are identified, maintained and prioritized.

8.2.1 Retention

Restricted PHI is retained in accordance with healthcare professional regulatory rules and CMPA retention recommendations

8.2.2 Labeling

Labeling of classified data is implied by the system where it is stored. Each data storage system is designed and configured with the appropriate controls for the classified data it contains. For instance, GitHub is the system of record for Source Code and shall be the primary storage where latest, stable, genuine code can be obtained for deployment. Of course, developer systems (laptops) can and will very often store a so-called “git clone” of various repositories, but deployment shall always be made using code that is auditable through GitHub.

When it comes to “Restricted PHI”, the most sensitive data classification at Dialogue, only the production Care Platform database and related subsystems shall store those records for as long as defined in 8.2.1. The Care Platform client application, during an active logged on session for an authorized licensed medical care professional, will temporarily store and process this class of data, but shall never retain it long term on the medical care professional's workstation device's disk (i.e. no data at rest). Upon logging out, data shall be purged from the workstation device's memory and disk cache.

Users of the various systems of record are expected to follow the simple rule that data originated in a given system shall not be copied to another one, except for moving data between the Care Platform and Electronic Medical Record (e.g. “Restricted PHI” stored in Care Platform shall not be copied to, for instance, Google Drive).

8.3 - Media handling

8.3.1. Removable media

(CC5.7)

The use of removable media (i.e. USB keys, external hard drives, etc.) is not authorized, with the sole exception of transfer of data between the Care Platform and an Electronic Medical Record. For any other exception, refer to the policy exception process (5.1.3) to evaluate acceptable temporary usage.

The use of unencrypted external storage devices is not allowed in any circumstance.

8.3.2 Disposal of media

(CC1.3)

Disposal of media that once stored data of a given class and is being considered for recycling or reallocation to another employee, shall be handled with great care. In the case of laptop computers, prior to reinstallation of the operating system and other software, secure data erasure must be performed. It is not sufficient to simply reformat the hard drive because sensitive data could still be retrieved after simple formatting. Secure data erasure shall, at a

minimum, completely overwrite the whole partition with zeros, ideally with random data. This option is available within personal computer operating system features or applications. Storage media that cannot be recycled shall be destroyed.

In the case of printed documents containing sensitive data, secure disposal must be done using an approved shredder that cuts diagonally the documents in small particles. The shredder shall be DIN 66399 Level P-4 compliant or better (i.e. particles less than 160mm^2, strips less than 6mm). Shredders with Level P-3 and below shall be avoided as reconstruction of the original document is possible by gluing strips back together.

9 - Access control

9.1 - Business requirements of access control

Business requirements of access control must align with this Information Security Policy. The purpose is to allow employees and contractors access to information and services they require to provide Dialogue service, while limiting access to only what's needed to fulfill the duties of a specific role. The decisions to authorize access follow a need-to-know principle. All access is forbidden unless explicitly permitted.

9.1.1 Access control policy
(CC5.1, CC5.3, CC5.4)
Access control is role-based and is applied to classes of data in accordance with the information classification defined by this policy. See also sections 6.1.1 and 8.2.

All business applications must include security requirements outlining specifications for the user roles required to access information.

Each access control request is recorded and submitted to Dialogue Identity Management (Okta) following an onboarding procedure. The access is revoked in accordance with the current offboarding procedure

Users can only access network resources they are authorized to use. Network access must be monitored and must use the secure wireless standard.

Access to production infrastructure must be done via Dialogue Identity Provider (Okta) Single Sign On using passwordless authentication mechanism.

9.2 - User access management

(CC5.2, CC5.3, CC5.4)
Internal users are authorized following the formal onboarding procedure, after the signature of all appropriate agreements. Each user is identified by a unique ID. Internal users shall be aware that account sharing is strictly prohibited, especially for any privileged administrative access. The only authorized exception would be for clearly designated low risk applications (such as for demo accounts, trial access to services, etc).

External users (members) must sign up for the service prior to receiving access. Each external user is identified by a unique user ID.

All user profiles are stored within a central registry (Auth0 for external users, Okta for internal users). Access to the registry is restricted to System Administrators. The registry maintains logs of successful and failed authentication attempts. Access logs are reviewed whenever the monitoring system triggers an anomaly alert.

9.2.1 Management of privileged access rights

Users with access to assets classified as Restricted PHI or Restricted Secret have additional controls.

Users with access to Restricted PHI via the Care Platform are restricted from accessing the infrastructure and Restricted PHI database. Users with access to a database are granted access to the minimum necessary database systems.

Privileged access rights are assigned to access control credentials and user ID different from those that are used for regular business activities.

Database credentials are generated when required and are valid for a period of 15 minutes. The credentials can only be generated by a user when authentication is done through Dialogue Identity Provider (Okta). Access to the database network itself is done through Cloudflare Zero-Trust tunnel. To be able to connect to a database a user must be granted the following:

1. Be an active user in the Identity Provider
2. Granted access to a database role via the Identity Provider
3. Granted access to the zero-trust tunnel via the Identity Provider
4. Granted access Cloudflare Access allowing network communication to the zero-trust tunnel

9.2.2 Management of secret authentication information of users

The authentication systems authorized to store authentication information are:

- Auth0 - for external users e.g. hr admins or members
- Okta - for internal users e.g. full time employees or contractors

Admin access to authentication systems is restricted to System Administrators.

All traffic to/from authentication systems is encrypted by a 2048-bit certificate issued by a trusted Certificate Authority over TLS v1.2.

9.2.3 Review of user access rights

Function owners and data owners must review access rights in an event of:

- Role change
- Termination
- Incidents
- Major changes in system architecture

9.2.4 Removal or adjustment of access rights

The access rights of all employees, contractors and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services are removed within one business day (using systems such as Okta). The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal of an account, password change, revocation or replacement of keys and external subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights.

In cases where the user's account is required to be active, the account may be temporarily suspended. Suspended accounts must be reviewed monthly by functional managers monthly and terminated as soon as they are no longer required.

9.3 - User responsibilities

9.3.1 Client user responsibilities

Dialogue's client users are responsible for:
1. Providing Dialogue with, and keeping up-to-date, a list of the individuals (Client HR Administrators) having authority to act on its behalf and updating Dialogue's system promptly of any departure of employees on that list;
2. Ensuring that creation, modification and removal of Dialogue member accounts are authorized and performed in a timely manner;
3. Restricting access to services provided by Dialogue to authorized client personnel;
4. Ensuring that user access credentials remain confidential;
5. Reporting to Dialogue in a timely manner any known or suspected incidents or problems with systems operation.

9.3.2 Member user responsibilities

Dialogue's member users are responsible for adhering to the Terms of Use agreed upon at the time of registration, which address responsibilities related to user accounts, minors and

dependants (if applicable), confidentiality, appropriate use of the platform, speech and conduct, software requirements, payments (if applicable).

9.4 - System and application access control

9.4.1 Secure log-on procedures

(CC5.3, CC5.4)

Where required by the access control policy, access to systems and applications is controlled by the secure log-on procedure:

- Does not display system or application details until the logon process has been successfully completed
- The log-on information is validated only on completion of all input data. Whenever the error arises, the system does not indicate which part of the data is correct or incorrect
- The system has the protection against brute-force login attempts. The security alert is emitted in case of repeated and excessive login attempts.
- The system does not display the password being entered.
- The system does not transmit log-on credentials in clear text
- For high-risk applications, the system terminates the logged-in sessions after a period of inactivity
- For systems giving access to restricted secret data, additional authentication measures are in place, such as ssh keys and multifactor authentication.

Google Workspace whitelist of apps to block phishing or granting access to Auth0.

9.4.2 Use of privileged utility programs

(CC5.1)

The use of utility programs that might be capable of overriding system and application controls is restricted. All uses of such tools produce an audit trail (CloudTrail, SSH access log).

- Admin utilities use identification, authentication and authorization procedure
- Admin utilities are segregated from application software
- Access to admin utilities is limited to the minimum practical number of trusted authorized users
- Ad-hoc authorization to utility programs is not allowed

9.4.3 Access control to program source code

(CC7.1, CC7.4)

Access to the source code of the Dialogue system is restricted to authorized users via Dialogue Identity Provider only.

Access to the source code and associated items (such as designs, specifications, verification plans and validation plans) is strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of intellectual property. The source code is stored in GitHub private repositories, the documentation is stored along with the code. The following guidelines are in place:

- The original source code is not available on production systems. All Dialogue systems are automatically deployed via an automated build process.
- Access to source code is granted explicitly to authorized users
- Complete audit logs of changes and updates are maintained.
- Source code updates are subject to change control procedures (see 14.2)

10 - Cryptography

Cryptography requirements are out of the scope of this policy given that they are covered by the security controls of Dialogue suppliers (AWS, Okta and Auth0) and outlined in the Dialogue Service and Security Overview document.

10.1 - Cryptographic controls

This section was deliberately left blank.

11 - Physical and environmental security

(CC5.5)

Dialogue uses Amazon Web Services and other 3rd party SaaS services to power its systems. All systems that store Restricted PHI must respect data sovereignty rules. All systems that store credit card information must be compliant with PCI-DSS.

No production systems are hosted in the physical Dialogue office. Dialogue does not operate an information processing facility (datacenter or a co-location facility).

11.1 - Secure areas

Individual phone booths are at the disposition of healthcare professionals and Service Operations staff for performing patient consultations. All open areas of the office are available to all employees and contractors, unless otherwise specified.

11.2 - Equipment

- Employee equipment is configured by the System Administrator to comply with the same level of security.
- Appendix A of the contractor agreement (“Technical Specifications and Data Policy”) defines the level of security of the contractor equipment.

12 - Operations security

12.1 - Operational procedures and responsibilities

(CC2.1, CC2.4, CC5.7, CC7.1, CC7.4)
Operational procedures for each critical component are developed and documented including

- Deployment
- Upgrades
- Monitoring
- Alerting

Processes are monitored following service level management procedures that monitor compliance with commitments and requirements.

Data assets classified as Restricted PHI and Restricted Secret are stored in encrypted form (encrypted at rest).

12.2 - Protection from malware

(CC5.8)
All company-owned computers (Mac, Windows) must be centrally managed via an MDM system (Kandji or Intune). Particularly, automated OS updates, firewall and default antivirus protection are enabled.

The malware, spam and phishing protection is installed on the email system (Google Workspace).

All endpoint devices used to access PHI are actively monitored by a security service such as Managed Security Service (SentinelOne). This includes personal devices owned by contractors. Failure to install SentinelOne on endpoint devices used to access company tools/systems could result in access being restricted unless an exception is granted by IT.

An Intrusion Detection System (IDS) has been implemented (AWS GuardDuty) to protect compute, storage and network resources and detect potential threats to Dialogue's cloud infrastructure security and Dialogue's endpoint.

12.3 - Backup

(CC6.1)
The primary production databases are managed by AWS RDS and AWS Backup, which has automatic backup as described in AWS documentation (https://aws.amazon.com/rds/faqs/ and https://aws.amazon.com/backup-restore/services/). Backups include incremental backups, full daily, weekly, monthly and yearly backups. Each of those backups have different retention

periods depending on the criticality of the data they stored. The backups are immutable by design and are protected against deletion from all users/roles including AWS root account user which is the highest privileged user on AWS.

Business documents are stored in Google Workspace, which also has automatic managed backups (https://support.google.com/a/answer/7376096).

12.4 - Logging and monitoring

(CC6.1)
Event logging sets the foundation for automated monitoring systems, which are capable of generating consolidated reports and alerts on system security. Event logs recording user activities, exceptions, faults and information security events are produced, kept and reviewed as needed. Logging and monitoring software is used to collect data from system infrastructure components and to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests. This software sends a message to the team. (CC3.2, CC4.1)

Successful and failed authentication attempts by anyone granted access to medical information are logged. Logs are transferred to Datadog for alerting purposes and kept for 15 days after which they are transferred back to AWS S3 for archiving where they are kept for 2 years. All access to infrastructure by sysadmins is logged, retained for 7 years in AWS Cloudtrails where they can be extracted and analyzed for forensic purposes.

Event logs include:
- user IDs
- system activities (authentication, access, failed attempt)
- dates, times and details of events
- Logs of sysadmin access to infrastructure include device identity or location if possible and system identifier
- records of successful and rejected system access attempts

The logs are classified as restricted secrets (see 8.2).

Monitoring and logging

- Events on Scoped Systems or systems containing Scoped Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents
- There is an automated system to review and correlate log and/or behavioral events (e.g., AWS GuardDuty)
- Personnel monitors security alerts related to Scoped Systems and Data at least daily
- All changes to user access rights logged on scoped systems and data

- Regular security monitoring include all changes to privileged user access rights on all scoped systems and systems with scoped data
- Regular security monitoring includes
  - Network IDS events
  - behavioral activity indicating botnet traffic
  - network device security events
  - server security events
  - application, Web Server, and Database security events
  - malware activity alerts such as uncleaned infections and suspicious activity
  - 24x7x365 security monitoring of the hosting environment

Dialogue has an established electronic monitoring policy which is posted in Notion.

12.5 - Control of operational software

(CC7.4)
12.5.1 Installation of software onto cloud environments includes deployment procedures.

The engineering team evaluates external dependencies to assure its continuous support. All external modules used by Dialogue systems are monitored for vulnerabilities (Mend Renovate - Whitesource, GitHub dependabot security alerts).

Security, privacy and risk considerations are evaluated as part of
a) software design
b) development and code review
c) test plan creation
d) testing.

12.5.2 Installation and downloads of software on Company owned End-User Devices

Dialogue expects all employees, contractors and temporaries to act with integrity when considering what, if any, non-core software or tools they may wish to use on their company-issued devices as the Company recognizes that there are non-core applications that are specialist, specific tools, adding additional value to employees and enabling them to best execute their roles and responsibilities.

In the event that any employee wishes to install a non-core application or service on company-issued devices, they must submit a Jira Ticket to the Information Technology team, specifying the details of the application or software, the service it is being intended to provide, and the details around the necessity of that requirement as pertains to their role and functional area within the Company.

This ticket is to be completed and submitted prior to the application or software being downloaded, and the IT team will review, assess and respond to that request. Whilst it is unlikely that this request will be denied, as the expectation is that all employees, contractors and temporary employees are acting with integrity and understanding of the needs for security within the organization, it will enable the Information Technology team to conduct due diligence and also then record the use of that asset within the broader Company ecosystem.

12.6 - Technical vulnerability management

12.6.1 Management of technical vulnerabilities
(CC3.3)
Appropriate and timely action must be taken in response to the identification of potential technical vulnerabilities:

- Desktop operating systems are set to default configuration to perform automated OS patching.
- System Administrators are responsible for vulnerability management of the infrastructure, including vulnerability monitoring, vulnerability risk assessment and patching.
- Software Developers are responsible for vulnerability management of the systems and applications, including vulnerability monitoring, vulnerability risk assessment and patching.
- Automated and active vulnerability monitoring is in place (Mend Renovate - Whitesource, GitHub Dependabot)
- HackerOne vulnerability bounty program.

13 - Communications security

13.1 - Network security management

(CC5.1, CC5.2, CC5.3, CC5.6, CC5.7)
This section defines the policy to ensure the protection of data in networks and its supporting data processing facilities

- System Administrators are responsible for maintaining and managing the network architecture
- Contractor suppliers provide basic internet connectivity to the office. AWS supplies connectivity to the production environment.
- All systems on the network are identified and access is authenticated. Connections are restricted.
- Network access to Dialogue systems is subject to monitoring
- Documented procedures are utilized for the installation and maintenance production servers and applications. The procedures include the use of an access control form to

grant access to authorized users. These procedures are reviewed at least annually and are communicated to appropriate IT personnel.

- Systems are configured to log access-related events. Systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.
- All network traffic to/from Dialogue Systems is encrypted by a 2048-bit certificate issued by a trusted Certificate Authority (AWS or Cloudflare).
- Administrative access privileges to key systems are restricted to authorized systems administration personnel via access group assignments.
- Appropriate segregation of duties is ensured through role-based access defined in the systems.
- Dialogue requires a **minimum** password baseline configuration for employees and for the following attributes:
    - password history;
    - minimum length (12);
    - complexity enforcement is enabled;
        - Use of a diversity of characters (uppercase, lowercase, numeric, does not contain part of username)
    - password reuse after (4);
    - password lockout (10 attempts).
- MFA (Multi Factor Authentication) enabled at organization level with factor enrollment and reset notifications. For all systems using Okta for identity authentication, MFA is enforced.
- Use of a password manager where a long (> 15 characters), fully randomized passphrase **is highly recommended in all scenarios** where the password does not need to be remembered by the user (i.e. all cases, except for computer logon and full disk encryption).
    - Dialogue strongly encourages the use of a password manager for employees and contractors.
- Network scans are performed for infrastructure elements to identify variance expected configuration.
- Changes in firewall configuration are reviewed and logged
- SSH access to database network zones (VPCs) are done through Cloudflare zero-trust tunnel.

13.2 - Information transfer

13.2.1 Confidentiality or nondisclosure agreements

(CC2.2, CC2.3, CC4.1)

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.

Dialogue's security commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal

system users to enable them to carry out their responsibilities. Specifically, client contracts may incorporate an IS appendix that describes Dialogue's commitments inline with the IS policy.

14 - System acquisition, development and maintenance

A system description is documented that includes the services provided, data, architecture, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is available to authorized internal and external users. (CC2.1)

14.1 - Security requirements of information systems

(CC3.1, CC7.2, CC7.4)
Security commitments and requirements are addressed during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.

The following steps are performed for major changes of Dialogue systems

1. Roadmap review. High-level security requirements are integrated in the high-level description of the change.
2. Design review. Design integrates authentication, error conditions and role-based access.
3. Sprint planning integrates security implementation as part of development of new features or updates.
4. Architecture review includes the focused review of the threat model in the context of the changes
5. Test plan includes test cases that assure security requirements are implemented
6. Development process uses best practices and secure coding guidelines
7. Unit testing includes tests to verify edge cases caused by unauthorized access
8. Integration testing exercises the changes in the context of external systems such as authentication system
9. Commit must pass static code analysis
10. Pull request documents the implementation changes
11. Continuous integration tests the pull request
12. Code coverage tool produces a code coverage report and alerts in case of the regression of the code coverage.
13. Peer code review validates the secure coding guidelines are respected
14. Deployment to the development environment validates the deployment process
15. User testing, integration testing validates the feature is implemented as expected
16. Deployment to production via automated procedure assures the production changes are performed completely and are logged.

All relevant technological choices that may have an impact on Information Security are captured and vetted by the CTO. Examples included selecting a cloud provider (AWS), setting up continuous monitoring and alerting (Datadog).

14.2 - Security in development and support processes

14.2.1 System change control procedures
(CC7.1, CC7.4)
Changes to Dialogue systems within the development lifecycle are controlled by the use of formal change control procedures. Introduction of new systems and major changes to existing systems follow a process of documentation, specification, analysis, testing, quality control and managed implementation and deployment.

The analysis step includes a risk assessment, analysis of the impacts of changes and specification of security controls, if needed. This step also ensures that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work.

The test activities are performed in an operational environment separate from production.

The deployment procedures are automated and do not require system administrators to utilize restricted access credentials to the production environment.

Management and users are notified of upcoming changes and maintenance activities that affect system security. Release notes are communicated to users through newsletters sent via e-mail, and maintenance notices are put in place via statuspage.io. Integrating user feedback and performing customer discovery activities are an integral part of product development process for the Care Platform and the Member App. Proposed system changes impacting customers may be reviewed with the customers through a User Testing platform on both the Care Platform and the Member App. A Care Platform Beta version is also available to receive early feedback upon upcoming changes. The system change calendar that describes changes to be implemented is posted on the intranet. (CC2.6)

15 - Supplier relationships

(CC7.1)
Critical external business partners selected by Dialogue adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization.

15.1 - Information security in supplier relationships

(CC1.2, CC3.2, CC2.3, CC5.8, CC7.4)
The critical supplier’s security commitments are documented in customer contracts. Critical suppliers must maintain equivalent level of controls as Dialogue or higher. System architecture review includes the review of the critical supplier systems and stated controls. System Administrators are responsible for tracking material updates and changes in critical supplier’s system properties or security policy.

Dialogue System is using Amazon Web Services (AWS), Auth0, Cloudflare, Datadog, Github, Google, InputHealth, Okta, SentinelOne, Sentry, UKG, Netsuite, IronClad, Azure as critical components. These systems meet or exceed controls stated in this policy, as stated by their compliance statements. Any material changes of the system architecture that would substitute these suppliers or any change to critical suppliers, must cause a full security review.

16 - Information security incident management

The Incident Response Team (IRT) works closely with the Engineering and Service Ops team to identify any potential concerns that would impair system security. The process is in place to identify members of the IRT, and their responsibilities.

16.1 - Management of information security incidents and improvements

(CC2.5, CC3.2, CC4.1, CC6.1, CC6.2, CC7.4)

The Data Security Incident Response Plan and Playbook ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

There is an established incident management program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program.

The Incident Response Plan consolidates privacy and cybersecurity incident response procedures, guidelines and tactics

Structure of Plan:

Document	Overview
Plan	- Summarized incident management program requirements - Delineates roles and responsibilities of Incident Response Cells (Exec Cell, Legal & Comms Cell, TechOps Cell) and any external parties involved in incident response (cybersecurity response vendor, external legal counsel specialized in cybersecurity response) - Outlines 8-step approach to cybersecurity incident response

Protocols and Guidance Attached to Plan	- Reporting and activation guidelines - Contact list - Cell communications protocols - General communications protocol - Evidence and record-keeping protocol - Privacy breach assessment guidelines, including (1) identification (2) evaluation (3) response procedure (4) reporting to Privacy Commissioner and notifying subject; and (5) investigation report template
Playbook	Tactical playbook covering common scenarios, leveraging and adapting Canadian Centre for Cyber Security and other regulatory guidance as well as lessons-learned from scenarios.

16.1.1 Summary of Responsibilities and procedures

- The CEO is responsible for formulating the company-wide response to the incident
- The CTO is responsible for reporting a technical description of the security incident. The CTO is the primary point of contact in an event of a security incident.
- The Engineering Team (Software Engineers, System Administrators) is responsible for analyzing security incidents.
- Account Managers are responsible for communicating with the affected clients.
- In case of an actual or attempted Security Incident the notification shall be prompt and no later than 4 hours of Dialogue having knowledge about the incident. Escalation procedure is in place.
- The affected clients shall be notified
- In cases where the security incident pertains to medical information, CMO (Chief Medical Officer) and CPO (Chief Privacy Officer) are responsible for communicating with patients and regulatory organizations as required.

All incidents are logged in Jira issues (tagged as minimum P1, security). In case the incident has a customer impact, it is also communicated via statuspage.io

The responsibility of System Administrators is to monitor external events (such as vulnerability reports) and assess their applicability and formulate a course of action (monitoring, patching, update, logging an improvement, raising a risk level, escalating to management).

A formal Incident Response Plan is in place and includes:

- guidance for escalation procedure
- procedures to collect and maintain a chain of custody for evidence during incident investigation
- feedback process to ensure those reporting information security events are notified of the results after the issue has been dealt with and closed.
- actions to be taken in the event of an information security event.
- formal disciplinary process for dealing with those who commit a security breach.
- a process for assessing and executing client and third party notification requirements (legal, regulatory and contractual)
- events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents

The Incident Response Plan requires:

- notifying the client when unauthorized access to Scoped Systems and Data is confirmed.
- identifying and mitigating all vulnerabilities that were exploited, removing all malware, inappropriate materials and other components, and remediating any affected systems discovered after incident closure
- returning systems to an operationally ready state, confirming that the affected systems are functioning normally and if necessary implement additional monitoring to look for future related activity
- notification procedures include any customer/client-specific notification requirements

The Incident Response Plan and changes to the plan distributed to defined stakeholders and organizations

Incident Reporting procedure

- Complete security event reporting form (Incident is logged in Jira and Post-Mortem in Notion) to support the reporting action and to help the person reporting remembering all necessary actions in case of an information security event
- Details about the event are noted immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact and taking only coordinated actions;
- Provide ongoing feedback processes to ensure that those persons reporting information security events are notified of results after the issue has been dealt with and closed.

(CC7.2, CC7.3) For high severity incidents, a root cause analysis is prepared and reviewed by operations management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect

the planned incident and problem resolution. Information security incidents are formally documented and communicated to appropriate internal and external users, as appropriate.

All incidents and defects are formally logged in Jira and receive a unique identifier.

Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.

16.1.2 Reporting information security weaknesses
(CC7.4)
Employees and contractors are required to note and report any observed or suspected weaknesses in systems or services. The reports should be done via private communication to one of the System Administrators via any secure communication channel (email, slack, Jira issue, in person). Employees who report the issue are still bound by this policy and shall not exercise or test the vulnerability. It is the responsibility of the System Administrators to validate the vulnerability.

An anonymous reporting system is also available via Officevibe and via the Whistleblower Policy and hotline.

17 - Information security aspects of business continuity management

(CC3.2)
Dialogue's Business Continuity Plan is in place.

The security policy remains valid even in cases of disaster, given that there is no dependency of physical access to the office to assure business continuity. See the teleworking section.

Dialogue Systems use a multi-zone deployment architecture that is capable of withstanding disasters affecting a given region.

18 - Compliance

18.1 - Compliance with legal and contractual requirements

18.2 - Information security reviews

The purpose of IS reviews is to ensure that security is implemented and operated in accordance with the Dialogue policies and procedures.

18.2.1 Independent review of information security

(CC7.1, CC7.4)

Dialogue's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently on a yearly basis or when significant changes occur.

Such a review shall be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews . Individuals carrying out these reviews should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the CISO who initiated the review. These records shall be maintained.

If the independent review identifies that the Dialogue's approach or implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see 5.1.1), SEMT shall consider corrective actions.

18.2.2 Compliance with the security policy

(CC7.1, CC7.4)

Function owners) shall regularly review the compliance of this Information Security Policy within their area of responsibility. Each function shall have a review process and cadence, but not less frequently than one year.

For every non-compliance, managers shall

- Identity the causes of non-compliance
- Notify the owner of the security policy
- Implement an appropriate corrective action
- Review the corrective action taken to verify its effectiveness

Results of reviews and corrective actions carried out by managers should be recorded, and these records should be maintained.

18.2.3 Technical compliance review

(CC7.1, CC7.4)

Technical compliance review shall be part of the architecture review (see 14.1).

Independent reviews and a penetration testing (pentest) shall be performed by an independent external organization at least yearly. Any external penetration testing should only be carried out by competent, authorized persons (such as Securis). The tests must follow best practices methodology.