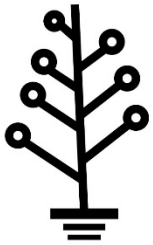

Data Security Plan

Aya Data Ltd

Table of Contents

1 EXECUTIVE SUMMARY 3

2 PURPOSE 3

3 SCOPE 3

4 DEFINITIONS 4

5 ICT GOVERNANCE COMMITMENTS & RESPONSIBILITIES 6

6 AYA DATA POLICY STATEMENT 7

7 ENFORCEMENT 7

8 INFORMATION SECURITY PROGRAM 8

8.1 Risk Assessment 8

8.2 Control Activities 8

8.2.1 Internal Controls 9

8.2.2 Preventative Controls 9

8.2.3 Detective Controls 9

8.2.4 Corrective Controls 9

8.3 Control Environment 10

8.3.1 Aya's Security Policy 10

8.4 Assets Accountability 11

8.5 Data Classification 11

8.5.1 TIER I: Public 11

8.5.2 TIER II: Internal 12

8.5.3 TIER III: Restricted 12

8.5.4 TIER IV: Confidential 12

8.6 Information Handling 12

8.7 Identity & Access Management 12

8.7.1 Identification 13

8.7.2 Authentication 13

8.7.3 Authorization 13

8.7.4 Remote Access 14

8.7.5 Privileged Access 14

8.7.6 Segregation Of Duties 15

8.8 Communication and Operations Management 15

8.8.1 Network Security 16

8.8.2 Security Monitoring 16

8.8.3 Encryption 16

8.8.4 Virus Protection 17

8.8.5 Backup And Recovery 17

8.9 Systems & Application Security 18

8.9.1 Systems Development and Maintenance 18

8.9.2 Change Control 19
8.10 Physical Security Measures 20
8.10.1 Physical Entry Controls 20
8.10.2 Provisioning Process 21
8.10.3 Visitors 21
8.10.4 Alarms & Surveillance 21
8.10.5 Equipment Control 21
8.10.6 Computer Data and Media Disposal Policy 21
8.11 Business Continuity 21
8.11.1 Business Impact Analysis 22
8.11.2 Disaster Recovery 23
8.12 Information Security Incident Response 23
9 Compliance Regulations 24
9.1 General Data Protection Regulation (GDPR) 24
9.2 Service Organization Controls II (SOC II) 24
9.3 ISO 27001 24
9.4 Health Insurance Portability and Accountability Act 25
9.5 Health Information Technology for Economic and Clinical Health Act 25
9.6 Gramm-Leach-Bliley Act for Disclosure of Nonpublic Personal Information 25
9.7 Red Flag Rules 25
9.8 Payment Card Industry Data Security Standards 25
10 Compliance 26
11 Related Policies & Procedures 26
12 DSP - Revision History 27

1 EXECUTIVE SUMMARY

Essential to the mission of Aya Data is Information security, an organizational-wide responsibility. The Aya Data Information Security Plan defines the information security standards and procedures for ensuring the privacy, confidentiality, integrity, and availability of all information systems resources and data under the control of Aya Data.

A Data Security Plan (DSP) is designed to protect information and critical resources from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information & Communication Technology (ICT) security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of Aya Data are met.

It is the responsibility of departments and individuals to uphold his plan. Inappropriate use exposes Aya Data to risks, including virus attacks, compromise of network systems and services, and legal issues. ICT security measures are intended to protect information assets and preserve the privacy of Aya Data's employees, clients, partners, sponsors, suppliers, and other associated entities.

All users of Aya Data's information technology resources are bound by this plan as well as other Aya Data policies and procedures as terms of their employment. All employees share responsibility for the security of the information and resources in their respective departments.

2 PURPOSE

The purpose of this security plan is to provide an overview of the security requirements of the ICT system and describe the controls in place or planned for meeting those requirements. Furthermore, Aya Data recognizes its responsibility to promote security awareness among the members of the Aya Data community. The security plan's objective is to improve ICT resources' protection.

3 SCOPE

This plan applies to the entire Aya Data community, including the Directors, Department Heads, Team Leads, employees, temporary employees, contractors, volunteers, and guests who have access to Aya Data information technology resources. Such assets include data, images, text, or software stored on hardware, paper, or other storage media.

4 DEFINITIONS

i. **Aya –** Aya Data Ltd.

ii. **ICT Resources -** All Aya Data computing systems, equipment, hardware, software, data, facilities, networks, and services supporting Aya's business activities.

iii. **Audit -** An independent, impartial examination of an information system to verify that it complies with its own rules. It is the technique of collecting and evaluating evidence of an organization's security practices and operations to ensure that an information system safeguards the organization's assets, maintains data integrity, and is operating effectively and efficiently to meet the organization's objectives.

iv. **Backup -** The process of copying data onto electronic storage media (i.e., backing up) that may then be used to restore the data to its original form after a data loss event or data file corruption. Two backup types are referenced in this document:

    1. Full-a complete backup of all data, whether or not changes have occurred

    2. Incremental-a backup of only those files that have changed or been added since the last full or incremental backup was performed.

v. **Confidentiality -** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

    A loss of confidentiality is the unauthorized disclosure of information.

vi. **Confidential Data or Records** - A private, proprietary, or otherwise sensitive nature.

vii. **Integrity** - Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.

    A loss of integrity is the unauthorized modification or destruction of information.

viii. **Privacy -** It concerns information about an entity and assures that this information is not made public or accessible by unauthorized parties or entities.

ix. **Availability** - Ensuring timely and reliable access to and use of information.

    A loss of availability is the disruption of access to or use of information or an information system.

x. **Data Classification -** The classification of the security level required for data within a record during the management, storage, and ultimate disposition of a record. Data with Restricted or Confidential classification per Aya Data's Classification policy must be secured at all times, including during the disposal process.

xi. **Disaster –** One of the following defines a disaster per this document:

    1. An emergency or other event resulting in data destruction, theft, or corruption.
    2. Extensive damage inflicted on an information system, the availability of which is necessary for maintaining confidentiality, integrity, privacy, and data availability required for an organization's operation.

3. The inability to access an information system and/or its data for longer than a reasonable period, the duration of which is determined by the criticality of the system resources and data.

xii. **Disaster Recovery -** The procedures, policies, and processes preparing for recovery or continuance of the technological infrastructure crucial to an organization after a natural or human-induced disaster. Disaster recovery includes planning for the resumption of the operation system, hardware, application software, data, and communications (networking).

xiii. **Threat -** Any circumstance or event that has the potential to intentionally or unintentionally exploit a particular vulnerability in the Aya System, resulting in a loss of confidentiality, integrity, privacy, or availability.

xiv. **Risk -** The probability that a particular vulnerability or vulnerabilities in the Aya information system will be intentionally or unintentionally exploited by a threat which may result in the loss of confidentiality, integrity, privacy, or availability, along with the potential impact of such a loss of confidentiality, integrity, privacy, or availability would have on Aya Data operations, assets, or individuals.

xv. **Risk Assessment –** It is a process that determines what information technology resources require protection and to understand and document potential risks from ICT security failures that may cause loss of information confidentiality, integrity, privacy, or availability.

xvi. **Control Activities –** These are the policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out.

xvii. **Information Assets -** Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to Aya Data.

xviii. **Access Control -** Refers to the process of controlling access to systems, networks, and information based on business and security requirements.

xix. **ISO (International Organization for Standardization) -** An international-standard-setting body composed of representatives from various national standards organizations.

xx. **NIST (National Institute of Standards and Technology) -** A non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

xxi. **VPN (Virtual Private Network) -** A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to Aya's network. VPNs use encryption and other security mechanisms to

ensure that only authorized users can access the network and that the data cannot be intercepted.

xxii. **IDS (Intrusion Detection System) -** A device (or application) that monitors the network and/or system activities for malicious activities or policy violations.

xxiii. **IPS (Intrusion Prevention System) -** A device (or application) that identifies malicious activities, logs information about these activities, attempts to block/stop activities, and reports activities.

xxiv. **Encryption -** Process of converting information so that it is humanly unreadable except by someone who knows how to decrypt it.

5 ICT GOVERNANCE COMMITMENTS & RESPONSIBILITIES

ICT governance is the responsibility of Executive Management and consists of the leadership, organizational structures, and processes to ensure that Aya's information technology sustains and extends Aya's strategies and objectives.

Executive Management has established the overall approach to governance and control by forming the Information Security Review Board (ISRB) to provide strategic direction, ensure objectives are achieved, ascertain risks are managed appropriately and verify that Aya's resources are used responsibly.

The Office of Data Protection and Compliance (ODPC) shows its commitment by developing and implementing good internal controls as well as ensuring the promotion and awareness of ICT standards and plans throughout the Organization. Aya's strategic vision is linked with the ICT department's goals and objectives, ultimately assuring that Aya Data meets customer and legal requirements while undergoing continual improvement.

5.1 Organization of Information Security

Aya Data assumes a coordinated approach to protecting information technology resources and depositories of protected information that are under its custody. This is attained by establishing appropriate and reasonable administrative, technical and physical safeguards that include all departments, individuals, or others that administer, install, maintain, or use Aya's information technology resources.

The ***Information Security Review Board's*** **(ISRB)** role is to provide oversight and direction regarding information systems security and privacy assurance across Aya Data.

The Office of Data Protection and Compliance **(ODPC)** is responsible for Aya's ICT planning, budgeting, and performance, including its information security components. Decisions made in these areas should be based on an effective risk management program.

The ODPC is also responsible for Aya's security programs, including GDPR, SOC II, and risk management and plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the information technology resources that support the Aya Data's mission and compliance needs.

Data Owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, privacy, and availability of information technology resources and data they own.

ICT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts) are responsible for adequately implementing security requirements within the information technology resources when change occurs.

Data Custodians have a responsibility to Aya Data to ensure they grant access to data to only those who require that access to perform their job responsibilities.

Data User is a person who has been granted explicit authorization to access the data by the owner. The user must use the data only for purposes specified by the owner, comply with security measures established by the owner or custodian (i.e., securing login-ID and password), and not disclose information or control over the data unless specifically authorized in writing by the owner of the data.

Third-Party Vendors providing hosted services and vendors providing support, whether on-site or from a remote location, are subject to Aya Data security policies and will be required to acknowledge this in the contractual agreements. The vendors are subject to the same auditing and risk assessment requirements as departments, and other units of Aya Data. All contracts, audits, and risk assessments involving third-party vendors will be reviewed and approved by the **ISRB** based on their area of responsibility.

Information Security Roles & Responsibilities. All Information Technology personnel and users with access to sensitive data are required to sign and date the *Confidentiality Agreement* at the time of hire, and annually thereafter.

6 AYA DATA POLICY STATEMENT

Each department will protect Aya's resources by adopting and implementing, at a minimum, the security standards and procedures developed and approved by the Information Security Review Board that are included within this DSP. Departments are encouraged to adopt measures that exceed the minimum requirements for protecting Aya's resources controlled exclusively within the department. All departments must meet the minimum standards.

Individuals within the scope of this policy are responsible for complying with this policy and the department's policy, if one exists, to ensure the security of Aya's resources.

7 ENFORCEMENT

All individuals accessing Aya Data's network resources and/or its working data must comply with local laws, regulatory laws (SOC 2, GDPR), and Aya Data policies and procedures regarding the security of sensitive data. Any Aya Data employee, partner, client, or non-Aya Data individual with access to Aya's network resources and/or data who engages in unauthorized use, disclosure, alteration, or destruction of data, violates this plan and will be subjected to appropriate disciplinary action, including possible dismissal and/or legal action.

8 INFORMATION SECURITY PROGRAM

Aya Data has established, documented, and implemented an Information Security Program through this document and associated policies. This program has been implemented to ensure the confidentiality, privacy, and integrity of Aya Data information while maintaining appropriate levels of accessibility. The system is designed to improve ICT operations' effectiveness and ability to satisfy regulatory requirements.

To ensure the security and confidentiality of sensitive information and to protect against any anticipated threats or hazards to the security or integrity of data, Aya Data has put in place all reasonable technological means (i.e., security software, hardware) to keep information and facilities secure. Aya Data has defined its security controls as equal to or greater than security requirements and controls prescribed by law and/or standards bodies (GDPR, SOC II, ISO, NIST, etc.).

8.1 Risk Assessment

A risk assessment is a process that determines what information resources require protection and to understand and document potential risks from ICT security failures that may cause loss of information confidentiality, integrity, or availability. A risk assessment aims to help management create appropriate strategies and controls for stewardship of information assets. Because economics, regulations, and operating conditions will continue to change, mechanisms are needed to identify and deal with the unique risks associated with change.

Objectives must be established before administrators can identify and take necessary steps to manage risks. Operations objectives relate to the effectiveness and efficiency of the operations, including performance and financial goals and safeguarding resources against loss. Financial reporting objectives pertain to the preparation of reliable published financial statements, including the prevention of fraudulent financial reporting. Compliance objectives pertain to laws and regulations which establish minimum standards of behaviour.

The Data Protection Officer (DPO), with the aid of other departments, will conduct an annual risk assessment and/or business impact analysis to:

- Inventory and determine the nature of Aya information resources
- Understand and document the risks in the event of failures that may cause loss of confidentiality, privacy, integrity, or availability of information resources
- Identify the level of security necessary for the protection of the resources.

8.2 Control Activities

Control activities are the policies, procedures, techniques, and mechanisms that help ensure management's response to reduce risks identified during the risk assessment process. In other words, control activities are actions taken to minimize risk. When the assessment identifies a significant risk to the achievement of an objective, a corresponding control activity or activities is determined and implemented.

Control activities occur throughout the organization at all levels and functions. They include various activities like approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

Control activities usually involve two elements: a policy establishing what should be done and procedures to affect the policy. All policies must be implemented thoughtfully, conscientiously, and consistently.

8.2.1 Internal Controls

Internal controls are designed to ensure that goals and objectives for the Organization and administrative areas are met. Adequate controls provide reasonable assurance regarding the accomplishment of established objectives.

Aya's internal controls, procedures, and practices also ensure that:

- Risks are reduced to an acceptable level
- All assets are safeguarded against waste, fraud, loss, unauthorized use or disclosure, and misappropriation
- Programs are efficiently and effectively carried out per applicable laws and Aya's policy

Controls are selected based on the cost of implementation relative to the reduction of risk and potential for loss if and when a security breach occurs. Non-monetary factors, such as reputation loss, are also considered.

The administrative processes within Aya Data rely on internal controls to comply with internal and external requirements. Sufficient controls to mitigate risks need to exist in everyday business procedures and can be preventative, detective, or corrective. Without adequate internal controls, functions within Aya Data may become non-compliant, inefficient, and too costly to operate, which in turn will ultimately fail.

8.2.2 Preventative Controls

Preventive controls are designed to discourage or pre-empt errors or irregularities from occurring. They are more cost-effective than detective controls. Credit checks, job descriptions, required authorization signatures, data entry checks, and physical control over assets to prevent improper use are all preventive controls utilized by Aya.

8.2.3 Detective Controls

Detective controls are designed to search for and identify errors after they have occurred. They are more expensive than preventive controls but still essential since they measure the effectiveness of preventive controls and are the only way to control certain types of errors effectively. Account reviews and reconciliations, observations, periodic physical inventory counts, passwords, transaction edits, and internal audits are examples of detective controls employed by Aya.

8.2.4 Corrective Controls

Corrective controls are designed to prevent the recurrence of errors. They begin when improper outcomes occur and are detected and keep the "spotlight" on the

problem until management can solve it or correct the defect. Quality teams' variance reports are examples of corrective controls used by Aya.

8.3 Control Environment

As established by Aya's management, the control environment sets the organization's tone and influences its people's control consciousness. Leaders of each department establish a local control environment. This is the foundation for all other components of internal control, providing discipline and structure.

Managers and employees are to have personal and professional integrity and maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.

This requires managers and their staff to maintain and demonstrate at all times:

- Personal and professional integrity and ethical values
- A level of skill necessary to help ensure effective performance
- An understanding of information security and internal controls sufficient to effectively discharge their responsibilities

Managers and supervisors are also responsible for ensuring their employees are aware of the relevance and importance of their activities and how they contribute to achieving the controll environment.

8.3.1 Aya’s Security Policy

The information technology resources at Aya Data support the organization's educational/training, administrative, research, and Business Process Outsourcing Services activities, and the use of these resources is a privilege extended to members of the Aya Data community. Any employee using Aya's information technology resources for any reason must adhere to strict guidelines regarding its use. Employees are being entrusted with the safety and security of Aya Data information resources. A sound security policy for information technology resources includes the participation of every employee at all times. A good policy promotes information security.

Any person or organization within the Aya Data community that uses or provides information technology resources has a responsibility to maintain and safeguard these assets. Each employee and management member in the Aya Data community is expected to use these shared resources with consideration for others.

Individuals are also expected to be informed and be responsible for protecting their own information resources in any environment, shared or stand-alone. It is unacceptable for anyone to use information resources to violate any law or Aya Data policy or perform unethical acts.

Aya’s Acceptable Use of Information Technology Resources contains the governing philosophy for effective and efficient use of Aya's computing, communications, and information resources by all members of the Aya Data community.

While directors and management are ultimately responsible for ensuring compliance with information security practices, the DPO, in cooperation with various department heads, will develop annual security awareness and compliance training to achieve technical proficiency and appropriate use for all employees.

8.4 Assets Accountability

Proper internal control is to be maintained over all information technology resources at all times. Adequate ICT asset management – from requisition to disposal – ensures a much greater likelihood that Aya Data will continue to meet customer requirements in the indefinite future by planning orderly fashion and mandating consistency throughout the organization.

ODPC will conduct an annual audit to ascertain the maintained registry of those members of the Aya Data community who have access to protected information and inventory of information assets on all Aya Data systems considered in scope. Individuals authorized to access organizational data shall adhere to the appropriate roles and responsibilities, as defined within contractual agreements and Aya's policies.

8.5 Data Classification

Data classification is required to determine the relative sensitivity and criticality of information technology resources, which provide the basis for protection efforts and access control. The Data Classification and Protection Standard establishes a baseline derived from best practices, state laws, regulations, and Aya Data policies that govern the privacy and confidentiality of data.

The Data Classification and Protection Standard apply to all data (e.g., client, partner, research, financial, and employee data collected in electronic or hard copy form that is generated, maintained, and entrusted to Aya Data). Except where a different standard is required by grant, contract, or the law.

All data within Aya must be classified into one of four sensitivity tiers or classifications that Aya Data has identified: Public, Internal, Restricted, and Confidential. Although all the enumerated data values require some level of protection, particular data values are considered more sensitive, and correspondingly tighter controls are necessary for these values.

All Aya's data is to be reviewed periodically and classified according to its use, sensitivity, and importance to Aya Data and in compliance with regulatory and/or state laws.

ODPC has pre-defined several types of sensitive data. The level of security required depends partly on the effect that unauthorized access or disclosure of those data values would have on Aya Data's operations, functions, image or reputation, assets, or the privacy of individual members of the Aya Data community.

8.5.1 TIER I: Public

This kind of information is accessible to the public. Making the information public will not damage the organization/client.

8.5.2 TIER II: Internal

This kind of information is accessible to every employee and authorized third parties. Unauthorized access may induce minor harm and/or inconvenience to the organization/client.

8.5.3 TIER III: Restricted

This kind of information is accessible to a specified group of employees and authorized third parties. Unauthorized access to information may cause substantial damage to the business and/or the organization's repute.

8.5.4 TIER IV: Confidential

This kind of information is accessible only to specified individuals in the organization. Unauthorized access to information could cause catastrophic damage to the business and/or the organization's repute.

8.6 Information Handling

Aya's employees create records as part of the ordinary course of conducting the organization's business. Records containing sensitive information should exist only in areas with a legitimate and justifiable business need and should be maintained under strict controls as outlined in this document.

Mishandling sensitive information is a significant risk to Aya Data and may cause considerable financial or reputational harm. All Aya Data employees, regardless of position, must protect sensitive information by being aware of any sensitive information they may store, process, or transmit.

The Data Classification and Protection Standard outlines the minimum standards for protecting sensitive Aya Data information. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health or financial information, credit card data), will be applied under specific circumstances.

8.7 Identity & Access Management

Identity and access management ensures accurate identification of authorized Aya Data community members and provides secure authenticated access to and use of physical and network-based services. Identity and access management is based on a set of principles and control objectives to:

- Ensure unique identification of members of the Aya Data community and assignment of access privileges
- Allow access to information resources only by authorized individuals
- Ensure periodic review of membership in the community and review of their authorized access rights
- Maintain effective access mechanisms through evolving technologies

Access Control refers to the process of controlling access to space, systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of Aya's information assets. Aya Data's access control measures

include secure and accountable means of identification, authentication, and authorization. Please see the Physical Office Security Policy for further reference.

8.7.1 Identification

Identification is the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about access levels. The key feature of an identification process is that each user of the Aya Data community, and any other entity about which access decisions need to be made, is uniquely identifiable from all other users.

8.7.2 Authentication

Authentication validates the identity of the person. The authentication process determines whether someone or something is who or what it is declared to be. Authentication factors can be something you know (password), something you have (token), or something you are (biometric). Two-factor authentication consists of two of the three factors (e.g., password and token) in these distinct categories. For access control, authentication verifies one's identity through ICT.

Passwords are an essential aspect of computer security. They are the front line of protection for user accounts. All community users (including directors, management, employees, guests, contractors, and vendors) are responsible for selecting and securing their passwords. A poorly chosen password may result in the compromise of Aya's entire network. Adhering to secure password procedures will help reduce the compromise of user accounts on Aya's systems. Please see Password Standards for further reference on passwords.

8.7.3 Authorization

Authorization is the process used to grant permissions to authenticated users. Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify).

The access rights to the information must then be entered into the security system via an access list, directory entry, or view tables, for example, so that the authorization rules can be enforced. The level of control will depend on the classification of the data and the level of risk associated with loss or compromise of the information.

In addition,

- The Data Owner must establish criteria for account eligibility, creation, maintenance, and expiration.
- The Data Owner must individually authorize sensitive data, and an annual confidentiality agreement must be acknowledged or signed by all authorized users.
- Depending on the relative sensitivity of the data, staff may be subject to a security clearance check before they are hired, transferred, or promoted. Any employee not subjected to such a clearance check when first hired should not be placed in a sensitive position until security clearance has been obtained.

- Data Owners must periodically review user privileges and modify, remove, or inactivate accounts when access is no longer required.
- Procedures must be documented for the timely revocation of access privileges and return of institutionally owned materials (e.g., keys, laptops) for terminated employees and contractors.
- Inactivity time-outs must be implemented, where technically feasible, for terminals and workstations that access sensitive data. The period of inactivity shall be no longer than 1 minute in publicly accessible areas.
- Audit trails exist for detective and reactive response to system penetration, infection of systems and data due to malicious code, catastrophic system loss, or a compromise of data integrity.

8.7.4 Remote Access

Remote access to information technology resources (switches, routers, computers, etc.) and sensitive or confidential information (social security numbers, credit card numbers, bank account numbers, etc.) are only permitted through secure, authenticated, and centrally-managed access methods. Systems that contain sensitive client, personnel, and financial data will be available for off-site remote access through an Aya centrally managed VPN that provides encryption and secure authentication.

It should also be understood that when accessing sensitive data remotely, storing any sensitive data onto local hard drives, floppy disks, or other external media (including laptops and Smartphones) is prohibited.

External computers used to administer Aya Data resources or access sensitive information must be secured. This includes patching (operating systems and applications), utilizing updated anti-virus software and firewall, with configurations as per all relevant Aya's policies and procedures.

8.7.5 Privileged Access

System administrators routinely require access to information resources to perform essential system administration functions critical to the continued operation of Aya Data. Such privileged access is often termed "root" or "administrator" access. Privileged accounts enable vital system administration functions to be performed and are only used for authorized purposes.

The number of privileged accounts is to be kept to a minimum and only provided to personnel whose job duties require it. Administrators or users who need privileged accounts should also have non-privileged accounts when performing daily routine tasks and should not use their privileged accounts for non-authorized purposes. Activities performed using a privileged account will be logged, and the logs will be reviewed regularly by an independent and knowledgeable person.

Personnel who manage, operate, and support Aya's information systems, including individuals who manage their own systems, are expected to use appropriate professional practices in providing for the security of the systems they manage. Responsibility for systems and application security must be assigned to an individual

knowledgeable about the information technology used in the system and in providing security for such technology.

8.7.6 Segregation Of Duties

Separate individuals must perform tasks involved in critical business processes. For example, the responsibilities of annotators, quality assurance teams, and system administrators must not overlap unless authorized by the Data Owner. Duties and obligations shall be assigned systematically to a number of individuals to ensure that effective checks and balances exist. Such controls keep a single individual from subverting a critical process. Essential duties include authorizing, approving, and recording projects, issuing and receiving assets, and reviewing or auditing projects.

Segregation of duties should be maintained between the following functions:

- Data annotation
- Quality assurance
- Data entry
- Computer operation
- Network management
- System Administration
- Systems development and maintenance
- Change management
- Security administration
- Security audit

Qualified and continuous supervision ensures that internal control objectives are achieved. This standard requires supervisors to continuously review and approve their staff's assigned work and provide the necessary guidance and training to ensure that errors, waste, and wrongful acts are minimized and that specific management directives are followed.

8.8 Communication and Operations Management

System communications protection refers to the critical elements used to assure data and systems are available and exhibit the confidentiality, privacy, and integrity expected by owners and users to conduct their business. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use it. The System's integrity controls must protect data against improper alteration or destruction during storage, processing, and transmission over electronic communication networks.

The critical elements of System and communications protection include backup protection, denial of service protection, boundary protection, use of validated cryptography (encryption), public access protection, and protection from malicious code.

Operations management includes implementing appropriate controls and protections on hardware, software, and resources, maintaining proper auditing and monitoring; and evaluating system threats and vulnerabilities.

Proper operations management safeguards Aya's computing resources from loss or compromise, including primary storage, storage media (e.g., tape, disk, and optical devices), communications software and hardware, processing equipment, standalone computers, and printers.

8.8.1 Network Security

Network attacks launched from the Internet or within Aya Data networks can cause significant damage and harm to information resources, including the unauthorized disclosure of confidential information. To provide defensive measures against these attacks, firewall and network filtering technology are implemented in a structured and consistent manner.

Aya Data maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network-mediated threats. Firewalls and Intrusion Detection Systems (IDS) are deployed at Aya's logical border. Intrusion Prevention Systems (IPS) are deployed on core services to augment standard system security measures to prevent denial of service attacks, malicious code, or other traffic threatening systems within the network or violating Aya's information security policies. Firewalls and/or IDS/IPS are also deployed to limit access to systems that host restricted or essential information.

8.8.2 Security Monitoring

Security Monitoring is a means to confirm that information resource security controls are in place, effective, and not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimize their impact on computer systems.

ODPC scans Aya's computer resources using commercial software to monitor and assess the security of Aya's network. Any equipment attached to Aya's network is subject to security vulnerability scans. The goal of the scans is to reduce the vulnerability of Aya Data computers and the network to hacking, denial of service, infection, and other security risks from both inside and outside the organization. Critical servers that store legally protected or other important non-public data are given priority, but others may be scanned.

ODPC also coordinates the external vulnerability scans for departments that are required to use this service, an example is to meet the Payment Card Industry Data Security Standards (PCI DSS) for credit card processing. The external scans must use a PCI-approved external scan vendor.

8.8.3 Encryption

Aya Data has developed standards for encryption to ensure that sensitive data is protected from disclosure. Suitably strong encryption measures are employed and implemented for information during transmission and storage, whenever deemed appropriate.

- ***Transmission***
  In order to protect the confidentiality, privacy, and integrity of Aya's sensitive data, any data classified as Tier IV or Tier III data shall be transmitted via not less than 256bit encrypted communication to ensure that it does not traverse the network in clear text.

- ***Storage***
  In order to protect the confidentiality, privacy, and integrity of Aya's sensitive data, any data classified as Tier IV or Tier III data shall be stored encrypted in systems and/or databases and/or portable media. See the Data Classification and Protection Standard for further clarification on data classification and handling.

8.8.4 Virus Protection

Viruses threaten Aya Data, as infected computers may transmit confidential information to unauthorized third parties, provide a platform for unauthorized access or use of the internal network, contaminate or infect other network-connected devices, or interfere with Aya Data information technology resources. Antivirus software is provided to the Aya Data community to protect against the damage caused by virus attacks. Network administrators are responsible for creating procedures to ensure antivirus software has the latest updates and virus signatures installed and verify that computers are virus-free.

Aya Data reserves the right to review any device (company-owned or non-company-owned) attached to its network for adequate virus protection. Aya Data reserves the right to deny access to the network to any device found to be inadequately protected. Additionally, Aya Data reserves the right to disable network access to any insufficiently protected device or is currently infected with a virus. Network access may be restored when the device has been cleaned, and current antivirus software, applicable operating system, and application patches have been installed.

8.8.5 Backup And Recovery

All electronic information must be copied onto secure storage media regularly (i.e., backed up) for disaster recovery and business resumption. The Backup and Recovery Standard outlines the minimum requirements for creating and retaining backups. Special backup needs which exceed these minimum requirements may be accommodated on an individual basis.

All backups must conform to the following best practice procedures:

- All data and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes, and updates)
- Records of what is backed up and to where must be maintained
- Records of software licensing should be backed up
- The backup media must be precisely labelled and must have, at a minimum, the following identifying markers that can be readily displayed by labels and/or a bar-coding system:

- System name
- Creation date
- Sensitivity Classification (Based on applicable electronic record retention regulations)

- Copies of the backup media, together with the backup record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site
- Regular tests of restoring data/software from the backup copies should be undertaken to ensure that they can be relied upon for use in an emergency. Note: For most important and time-critical data, a mirror system, or at least a mirror disk may be needed for a quick recovery.

8.9 Systems & Application Security

Application development procedures are vital to the integrity of systems. If applications are not developed properly, data may be processed in such a way that the integrity of the data is corrupted. In addition, the integrity of the application software itself should be maintained, both in terms of change control and terms of attack from malicious software.

8.9.1 Systems Development and Maintenance

Security has to be considered at all stages of the life cycle of an information system to: a) ensure conformance with all appropriate security requirements, b) protect sensitive information throughout its life cycle, c) facilitate efficient implementation of security controls, d) prevent the introduction of new risks when the system is modified, and e) ensure proper removal of data when the system is retired.

To ensure that systems security is considered during the development and maintenance stages, Aya Data has defined a Systems Development Lifecycle (SDLC) and the following minimum requirements during each phase:

- **Feasibility Phase** – high-level review to ensure security requirements can support the business case
- **Requirements Phase** – define any initial security requirements or controls to support the business requirements
- **Design Phase** – verify appropriate security controls for the baseline have been identified and ensure change control is established and used for the remainder of the life cycle. Repeat verification with each design change or as warranted
- **Development Phase** – to verify and validate all security controls identified from the design phase. Repeated throughout as changes are made or as warranted
- **Implementation Phase** – final verification of existing controls and the appropriate levels of risk mitigation

8.9.2 Change Control

Change Control is the process that management uses to identify, document, and authorize changes to an ICT environment. It minimizes the likelihood of disruptions, unauthorized alterations, and errors.

The change control procedures are designed with the size and complexity of the environment in mind. For example, complex applications maintained by a large ICT staff or representing high risks require more formalized and more extensive processes than simple applications maintained by a single ICT person. In all cases, there should be clear identification of who is responsible for the change control process.

Aya Data has a change management policy with the following elements included:

- **Change Request Initiation and Control** - Requests for changes must be standardized and subject to management review. Changes are categorized and prioritized, and specific procedures are in place to handle urgent matters. Change requestors should be kept informed about the status of their request.
- **Impact Assessment** - A procedure is in place to ensure that all change requests are assessed in a structured way for all possible impacts on the operational system and its functionality.
- **Control and Documentation of Changes** - Changes to production systems are made only by authorized individuals in a controlled manner. Where possible, a process for rolling back to the previous version should be identified. It is also essential to document what changes have been made. At a minimum, a change log should be maintained that includes:
    - A brief functional description of the change
    - Date the change was implemented
    - Who made the change
    - Who authorized the change (if multiple people can authorize changes)
    - What technical elements were affected by the change e.g., program modules, database tables or fields, screens and forms
- **Documentation and Procedures** - The change process includes provisions that the associated documentation and procedures are updated whenever system changes are implemented.
- **Authorized Maintenance** - Staff maintaining systems must monitor specific assignments and their work as required. In addition, their system access rights should be controlled to avoid risks of unauthorized access to production environments.
- **Testing and User Signoff** - Software is thoroughly tested for the change itself and the impact on elements not modified. A standard suite of tests should be developed as well as a separate test environment. The standard test suite will help identify if core elements of an application were inadvertently affected. Data

owners of the systems should be responsible for signing off and approving changes being made.

- **Testing Environment** - Ideally, systems should have at least three separate environments for development, testing, and production. The test and production environments should be as similar as possible, except for size. If cost prohibits having three environments, testing and development may occur in the same environment; but development activity needs to be closely managed (stopped) during acceptance testing. In no case should untested code or development be in a production environment.

- **Version Control** - Control is placed on production source code to ensure that only the latest version is being updated. If not, previous changes may be inadvertently lost when a new change is moved into production. Version control may also help to effectively back out of a change that has unintended side effects.

- **Emergency Changes** - Emergencies may occur that require some of the program change controls to be overridden, such as granting programmers access to production. However, at least a verbal authorization should be obtained, and the change should be documented.

- **Distribution of Software** - As a change is implemented, all components of the change must be installed in the correct locations and on time.

- **Hardware and System Software Changes** - Changes to hardware and system software should also be tested and authorized before being applied to the production environment. They should also be documented in the change log.

If a vendor supplies patches, they should be reviewed and assessed for applicability and potential impact to determine whether the system requires their fixes.

8.10 Physical Security Measures

Physical security controls and secure areas minimize unauthorized access, damage, and interference to information and information systems. Physical Security means providing environmental safeguards for controlling physical access to equipment and data within the Aya Data community to protect information technology resources from unauthorized use, in terms of both physical hardware and data perspectives.

8.10.1 Physical Entry Controls

Access to areas containing sensitive information must be physically restricted. Electronic access control mechanisms protect access to all entry points into and within Aya Data's environment to validate access and ensure that only authorized individuals enter the facility. An audit trail of all access is securely maintained for auditing purposes.

All individuals with access to these areas must wear an identification badge on their outer garments so that the picture and information on the badge are clearly visible. Individuals are also encouraged to challenge unescorted strangers and anyone not wearing visible identification. Access rights to secure areas are regularly reviewed and updated.

8.10.2 Provisioning Process

Individuals requesting access to the premises of Aya Data are to be enrolled in a structured and documented provisioning process to ensure the integrity of the person entering the facility.

Personnel working within Aya's facility or clients utilizing the facility services must be immediately removed from systems that have allowed access to the facility when no longer employed by Aya Data. This includes all electronic access control mechanisms and the removal from all systems, databases, Web portals, or any other sign-in mechanism requiring authentication and authorization activities.

8.10.3 Visitors

Visitors must be correctly identified with a current, valid form of identification and given a temporary facility badge allowing access to certain areas within the facility. A log of this activity is retained for audit and security purposes.

8.10.4 Alarms & Surveillance

All exterior doors and sensitive areas within the facility are hard-wired with alarms. They have a mixture of security cameras throughout all critical areas, both inside and out, of the facility.

8.10.5 Equipment Control

Sensitive information technology resources located in unsecured areas should be secured to prevent physical tampering, damage, theft, or unauthorized physical access. The assigned user of an information technology resource is considered the custodian of the resource. If the item has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform the involved department manager.

An inventory of all computer equipment and media is maintained. ICT devices are to be marked with some form of identification that clearly indicates it is the property of Aya Data.

8.10.6 Computer Data and Media Disposal Policy

Proper data disposal is essential to controlling sensitive data, including client, partner, personnel records, financial, research data, and protected health and credit card information. Suppose the information on those systems is not properly removed before the equipment is disposed of or transferred within Aya Data. In that case, unauthorized individuals could access and view that information.

Media or devices containing sensitive information transferred between departments or removed from service must be adequately sanitized, as outlined within the Aya Data E-waste Policy, to ensure that all computers and electronic media are adequately sanitized before disposal. Aya Data is committed to compliance with regulatory statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements.

8.11 Business Continuity

Aya Data provides a safe, secure ICT environment to serve its customers' requirements, ensure stability and continuity of the business, and promote confidence in its ability to provide services and recover quickly from disaster to minimize disruption.

8.11.1 Business Impact Analysis

A Business Impact Analysis should correlate specific system components with the critical services they provide and, based on that information, characterize the consequences of a disruption to the system components. Both the Data Owner and Data Custodian are responsible for performing appropriate business impact analysis tasks as outlined below.

Identify Critical ICT Resources

Data owners and custodians are to evaluate their systems to determine the critical functions performed and identify the specific system resources required. Two activities usually are needed to complete this step:

1. Identify and coordinate with internal and external users associated with the system to characterize how they depend on or support the system. When identifying contacts, it is vital to include departments that provide or receive data from the system and contacts supporting any interconnected systems. This coordination should enable the data owner and custodian to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

2. Evaluate the system to link these critical services to system resources. This analysis usually will identify infrastructure requirements such as electric power, telecommunications connections, and environmental controls. Specific ICT equipment, such as application servers, and authentication servers, are usually considered to be critical. However, the analysis may determine that certain ICT components, such as printers or print servers, are not needed to support critical services.

Identify Outage Impacts and Allowable Outage Times

Data owners and custodians should analyze the critical resources identified in the previous step and determine the impact(s) on ICT operations if a given resource is disrupted or damaged. The analysis should evaluate the effect of the outage in the following three ways:

1. The effects of the outage may be tracked over time. This will enable Aya Data to identify the maximum allowable time that a resource may be unavailable before it prevents or impedes the performance of an essential function.

2. The outage effects may be tracked across related resources and dependent systems, identifying any cascading effects that may occur as a disrupted system affects other processes that rely on it.

3. The effects of the outage may be tracked using revenue streams and cost expenditures, identifying any areas of financial need or concern that could cause a delay in the recovery effort.

Data owners and custodians will determine the optimum point to recover the ICT system by balancing the cost of system inoperability against the cost of resources required for restoring the system.

Develop Recovery Priorities

Data owners and custodians should develop recovery priorities for the system resources. A high-, medium-, or low scale should be used to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a more extended recovery period.

The outage impact(s) and allowable outage times characterized in the previous step enable Aya Data to develop and prioritize recovery strategies that personnel implement during contingency plan activation. By prioritizing these recovery strategies, Aya Data may make more informed, tailored decisions regarding contingency resource allocations and expenditures, saving time and effort. For example, if the outage impacts step determines that the system must be recovered within 4 hours, Aya Data must adopt measures to meet that requirement. Similarly, if most system components could tolerate a 24-hour outage, but a critical component could be unavailable for only 8 hours, the necessary resources for the critical component would be prioritized.

Business Impact Analysis Documentation Requirements

Data owners and custodians are responsible for maintaining the Business Impact Analysis document(s). The data owner should periodically review the Business Impact Analysis to ensure accuracy and completeness.

8.11.2 Disaster Recovery

A disaster recovery plan can be defined as the ongoing process of planning, developing, and implementing disaster recovery management procedures and techniques to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

The main components of the disaster recovery plan are documented in the Business Continuity Document, which provides essential information to ensure a comprehensive plan, Notification/Activation, Recovery, and Reconstitution following a system disruption or emergency.

The Disaster Recovery Plan contains detailed information on how to continue business operations and perform all required tasks while the computer hardware, network, and data are recovered. Technical capabilities must be documented, designed to support operations, and tailored to Aya's requirements. The order in which systems are to be recovered and the level of functionality based upon the business impact analysis needs to be fully documented. Not all systems may need to be recovered simultaneously or to 100% to begin functioning.

8.12 Information Security Incident Response

An ICT security incident is defined as an event that impacts or potentially impacts the confidentiality, availability, or integrity of Aya's information technology resources. Proper handling of such incidents protects Aya's information technology resources from future unauthorized access, use or damage. Effective incident response is essential in mitigating damage and loss due to an information security incident.

If you suspect an ICT security incident, immediate action should be taken to isolate the problem from Aya's network. Be ready to provide specifics such as date/time of loss, type of device(s), contact information, and any specific information that you believe indicates that a device was breached, a computer security incident occurred, or a device was lost or stolen. Please see the ICT Incident Response Procedure for further reference.

9 Compliance Regulations

Aya's information security practices must comply with various international and state laws and its own internal policies. These laws and policies are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. These include personally identifiable information (e.g., social security numbers), personal financial information (e.g., credit card numbers), health information, and other confidential information.

Among the laws and regulations that mandate baseline privacy and information security controls for Aya's Information Security Program, the most notable include the following:

9.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for collecting and processing personal information from individuals living in the European Union (EU). GDPR governs Aya's collection and processing of personal information from individuals.

The GDPR mandates that EU visitors be given several data disclosures. Aya Data must facilitate such EU consumer rights as a timely notification if personal data is breached.

9.2 Service Organization Controls II (SOC II)

SOC 2 or Service Organization Controls were developed by the American Institute of CPAs (AICPA). They are based on five trust services criteria: security, availability, processing integrity, confidentiality, and privacy. Aya Data applies these five trust services criteria in setting up its internal controls, thereby addressing the risk associated with its outsourced services.

On a yearly basis, Aya Data undergoes an independent SOC 2 audit with a certified audit firm. The final audit report is made available to the public.

9.3 ISO 27001

ISO/IEC 27001 is a leading international standard for regulating data security through a code of practice for information security management.

ISO/IEC 27001 is comprised of a set of standards covering different aspects of information security. Aya Data adheres to these standards, including information security management systems, information technology, information security techniques, and information security requirements.

9.4 Health Insurance Portability and Accountability Act

HIPAA and its regulations (the "Privacy Rule" and the "Security Rule") protect the privacy of an individual's health information as well as govern the way Aya Data collects, maintains, uses, and discloses protected health information ("PHI").

Aya Data must ensure the confidentiality, privacy, integrity, and availability of confidential information; and detect and prevent reasonably anticipated errors and threats due to malicious or criminal actions, system failure, natural disasters, and employee or user error. Such events could result in damage to or loss of personal information, corruption or loss of data integrity, interruption of Aya's activities, or compromise of the privacy of Aya's employees and records.

9.5 Health Information Technology for Economic and Clinical Health Act

HITECH imposes United States federal security breach notification requirements for unauthorized uses and disclosures of "unsecured PHI" and adds numerous privacy and data security restrictions to HIPAA.

9.6 Gramm-Leach-Bliley Act for Disclosure of Non-public Personal Information

GLBA mandates that Aya Data safeguard non-public personally identifiable financial information (PIFI); limit disclosures of such data, and notify customers of their information-sharing practices and privacy policies. The act states, among other things, that Aya Data must develop, implement and maintain a written comprehensive information security program. The plan must be "reasonably designed" to achieve the security and confidentiality of customer data, to protect against anticipated threats or hazards, and protect against unauthorized access or use that could result in substantial harm. It must contain administrative, technical, and physical safeguards appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the relevant customer data.

9.7 Red Flag Rules

The RFR requires that Aya Data implement a written Identity Theft Prevention Program designed to detect the warning signs – or "red flags" – of identity theft in their day-to-day operations. By identifying red flags in advance, businesses will be better equipped to spot suspicious patterns that may arise and take steps to prevent a red flag from escalating into a costly episode of identity theft.

9.8 Payment Card Industry Data Security Standards

A framework of standards and compliance requirements designed to protect consumer payment card data. PCI DSS provides a single approach to safeguarding confidential credit card account data and establishes security best practice standards Aya Data must follow when storing, processing, or transmitting credit card data. Aya Data must comply to be approved and continue to accept payment cards.

10 Compliance

Upon implementing this plan, ODPC will ensure that the plan is being effectively carried out per regulatory and Aya's requirements to meet or exceed industry standards for information security.

11 Related Policies & Procedures

Aya Data Code of Conduct
Aya Data Security Policies Summary
Business Narratives

Below are the policies under the *Privacy Preserving Policies Document*:
Data Classification Policy
Confidentiality Policy
Logging Management Policy
Physical Office Security Policy
Data Retention Policy
Risk Assessment Policy
Data Anonymisation and Pseudonymisation Policy

Below are the policies under the *Data Protection and Security Policies Document*:
Network/Server Security Policy
Workstation Security Policy
Password Security Policy
Acceptable Use
Encryption Policy
e-mail Policy
Metadata Policy
Remote Access Policy
Employee termination Policy
Visitor and Contractor Access Policy

Below are the policies under the *Business Continuity Policies Document*:
Availability Policy
Disaster Recovery Policy
Incident Reporting Policy
System Change Policy
Training and Development Policy

Below are the policies under the *Environmental Policies Document*:
Clean Desk Policy
E-waste Policy

12 DSP - Revision History

Revision	Date	Description of changes	Requested By
Rev 2	12/06/2022	Final Version	DPO