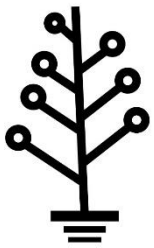
DATED August 2021



Privacy Preserving Policies

Aya Data Ltd

Table of Contents

1 Data Classification Policy

1.1 Purpose and Scope

a) The data classification policy specifies the requirements to ascertain that information in the organization is safeguarded at an appropriate level.
b) This document concerns the entire scope of the organization's information security program. It incorporates all types of information, regardless of its forms, particularly paper or electronic documents, applications and databases, and knowledge or information not written.
c) This policy is relevant to all individuals and systems that have access to information held by the organization.

1.2 Background

This policy specifies the high-level aims and implementation instructions for the organization's data classification scheme. This comprises data classification levels and procedures for classifying, labelling, and handling data in the organization. Confidentiality and non-disclosure agreements held by the organization should reference this policy.

1.3 The Policy

a) If classified information is obtained from outside the organization, the individual who receives it must classify it by the rules directed in this policy. The person thereby becomes the owner of the information.
b) If classified information is obtained from outside the organization and handled as part of business operation activities (e.g., client data on provisioned cloud services), the information classification, as well as the owner of such information, must be done per the terms of the corresponding customer service agreement and other legal requirements.
c) During information classification, the level of confidentiality is decided by:
    i. The value of the information on the basis of impacts identified during the risk assessment procedure. Further information on risk assessments is defined in the Risk Assessment Policy (Risk Assessment Policy).
    ii. The information's sensitivity and criticality are based on the highest risk calculated for each information item during the risk assessment.
    iii. Legal, regulatory and contractual obligations.

Information Confidentiality Levels:

Confidentiality Level	Label	Classification Criteria	Access Restriction
Public	For Public Availability	Making the information public will not damage the organization/client in any way.	Information is accessible to the public
Internal Use	Internal Use	Unauthorized access may induce minor harm and/or inconvenience to the organization/client.	Information is accessible to every employee and authorized third parties.
Restricted	Restricted	Unauthorized access to information may cause substantial damage to the business and/or the organization's repute.	Information is accessible to a specified group of employees and authorized third parties.
Confidential	Confidential	Unauthorized access to information could cause catastrophic damage to the business and/or the organization's repute.	Information is accessible only to specified individuals in the organization.

d) Information should be classified based on confidentiality levels as defined above.
e) Information and information system owners must try to utilize the lowest confidentiality level that ascertains an adequate level of protection, thereby preventing unnecessary production costs.
f) A list of authorized persons must accompany information classified as "Restricted" or "Confidential." The information owner must specify the names or work functions of persons who possess the right to access that information.
g) Information classified as "Internal Use" should be supplemented by a list of authorized persons only if individuals outside the organization would have access to the document.
h) Information and information system owners should review the confidentiality level of their information assets annually and assess whether or not the confidentiality level must be changed. Wherever feasible, confidentiality levels should be lowered.
i) For cloud-based software services offered to clients, system owners under the company's control must also review the confidentiality level of their information systems following a service agreement change or after a client's formal notification through writing. Where permitted by service agreements, confidentiality levels should be lowered.
j) Information should be labeled in compliance with the following:
    i. **Paper documents**: the confidentiality level is declared on the top and bottom of each document page; it is also exhibited on the front of the cover or envelope carrying such a document and on the filing folder in which it is stored. If a document is not labeled, by default, its classification is Internal Use.
    ii. **Electronic documents**: the confidentiality level is declared on the top and bottom of each document page. If a document is not labeled, by default, its classification is Internal Use.
    iii. **Information systems**: applications and databases confidentiality level should be declared on the system access screen.
    iv. **Electronic mail**: the confidentiality level is declared in the first line of the email body. If it is not labeled, by default, its classification is Internal Use.
    v. **Electronic storage media** (USB drives, memory cards, etc.): the confidentiality level must be declared on the upper surface of the media. If it is not labeled, by default, its classification is Internal Use.
    vi. **Information conveyed orally**: the confidentiality level must be stated before having a face-to-face information discussion, telephone, or any other means of verbal communication.
k) All persons accessing classified information must observe the instructions listed in “Procedure For Handling of Classified Information”.

l) Incidents associated with the inappropriate handling of classified information must be reported per the Incident Reporting Policy.

1.4 Procedure For Handling of Classified Information

Information and information systems should be handled according to the following guidelines:

a) **Paper Documents**.

i. Internal Use.

1. Only authorized persons may have access.
2. If dispatched outside the organization, the document should be posted as registered mail.
3. Documents may only be filed in rooms without public access.
4. Documents must be removed promptly from printers and fax machines

ii. Restricted.

1. The document should be filed and kept in a locked cabinet.
2. Documents may be transmitted within and outside the organization only in a sealed envelope.
3. If sent outside the organization, the document should be posted with a return receipt service.
4. Documents must be swiftly removed from printers and fax machines.
5. Only the document owner may duplicate the document.
6. Only the document owner might destroy the document.

iii. Confidential.

1. The document should be filed and kept in a safe.
2. The document may be transmitted within and outside the organization only by a reliable person in a sealed envelope.
3. Faxing the document is prohibited.
4. The document could be printed only if the authorized person is the only one doing the printing.

b) **Electronic Documents**.

i. Internal Use.

1. Only authorized persons may have access.
2. When documents are conveyed via unencrypted file-sharing services such as FTP, they must be password guarded.
3. Access to information systems where the document is located must be protected by a secure password (According to the password policy).
4. The displayed screen on which the document is, should be locked automatically after 2 minutes of inactiveness.

ii. Restricted.

1. Only persons with authorized access to this document may access the information system section where this document is stored.
2. When documents are exchanged via file-sharing services of any type, they must be encrypted.
3. Only the document owner may delete the document.

iii. Confidential.

1. The document must always be stored in encrypted form.

2. The document may be kept only on servers that the organization controls.
3. The document may only be shared via file-sharing services that are encrypted, such as HTTPS and SSH. Moreover, the document must be encrypted and protected with a strong password when transmitted.

c) **Information Systems**.

i. Internal Use.

1. Only authorized persons may have access.
2. A strong password must protect access to the information system.
3. The screen must be automatically locked after 2 minutes of inactiveness.
5. The information system may be only situated in rooms with controlled physical access.

ii. Restricted.

1. All users must log out of the information system if they have temporarily or permanently left the workplace.
2. Data should be erased with only approved algorithms that ensure secure deletion.

iii. Confidential.

1. Access to information systems must be controlled utilizing multi-factor authentication (MFA).
2. The information systems may only be installed on servers managed by the organization.
3. The information systems may only be located in rooms with controlled physical access and identity control of people accessing the space.

d) **Electronic Mail**.

i. Internal Use.

1. Only authorized persons may have access.
2. The sender must carefully check the recipient.
3. All rules stated under "**Information Systems**." apply.

ii. Restricted.

1. Email should be encrypted if sent outside the organization.

iii. Confidential.

1. Email must be encrypted.

e) **Electronic Storage Media**.

i. Internal Use.

1. Only authorized persons may have access.
2. Media or files must be password protected.
3. If dispatched outside the organization, the storage media must be sent as registered mail.
4. The medium may only be stored in rooms with physical controlled access.

ii. Restricted.

1. Media and files must always be encrypted.

2. Media must be kept in a locked cabinet.
3. If dispatched outside the organization, the medium must be posted with a return receipt service.
4. Only the medium owner may delete files or destroy the medium.

iii. Confidential.
1. Media must be kept in a safe.
2. Media may be transmitted within and outside the organization only by a reliable person and in a sealed envelope.

f) **Information Transferred Orally**.
i. Internal Use.
1. Only authorized persons should have access to information.
2. Unauthorized persons must not be available in the room when the information is communicated.

ii. Restricted.
1. The room must be soundproof.
2. The conversation should not be recorded.

iii. Confidential.
1. Conversations conducted through electronic resources must be encrypted.
2. No transcript of the conversation should be kept.

With this document, controls are enforced cumulatively; in other words, controls for any confidentiality level signify the implementation of controls established for lower confidentiality levels. If stricter controls are stipulated for a higher confidentiality level, then only such controls are executed.

2 Confidentiality Policy

2.1 Purpose and Scope

a) This policy outlines the expected behavior of employees to keep confidential information about clients, partners, and our company secure.

b) This policy is applicable to all levels of employees, board members, investors, and contractors, who may access confidential information. This policy is to be made readily available to all whom it applies.

2.2 Background

a) The company's confidential information should always be protected for two reasons:
i. It may be legally binding (i.e., sensitive client data)
ii. It may be a fundamental business objective(i.e., business processes)
b) Common examples of confidential information in our organization include, but is not restricted to:
i. Client/partner/vendor/external party data
ii. Unpublished financial information

iii. New technologies, patents, formulas, and other intellectual property
iv. Current and potential client lists
v. Unrevealed business strategies, including pricing & marketing
vi. Materials & processes that are explicitly tagged as "confidential."

c) Employees will have differing levels of accredited access to confidential information.

2.3 The Policy

a) *Employee procedure for handling confidential information*
   i. Lock and secure, confidential information all the time
   ii. Securely discard of (i.e., shred) documents when no more needed
   iii. View confidential information on secure devices only
   iv. Reveal information only when authorized and necessary
   v. Do not utilize confidential information for personal gain, advantage, or profit
   vi. Do not reveal confidential information to persons outside the company or to anyone within the company who does not possess appropriate authorizations
   vii. Do not keep confidential information or replicate confidential information in unsecured manners (i.e., on unsecured devices)
   viii. Do not remove confidential documents from the company's premises unless necessary to move.

b) *Off-boarding measures*
   i. The Hiring Manager must confirm the off-boarding procedure has been completed by the final date of employment.

c) *Confidentiality measures*.
   i. The company will take the following step to guarantee the safeguard of confidential information:
      1. Store and keep under lock paper documents
      2. Encrypt electronic information and execute appropriate technical measures to safeguard databases
      3. Require employees to sign non-disclosure/non-compete agreements
      4. Confer with senior management before giving employees access to specific confidential information

d) *Exceptions*
   i. Under given legitimate conditions, confidential information may require to be disclosed. Examples include:
      1. If a regulatory authority requests information as part of an audit or investigation activity
      2. If the organization needs disclosing information (within legal boundaries) in the course of a venture or partnership.
   ii. In such instances, employees must request and receive written approval from their hiring manager before revealing confidential information to a third party.

e) *Disciplinary consequences*
   i. Employees found to breach the confidentiality policy will face disciplinary and potential legal action.
   ii. A suspected violation of this policy will prompt an investigation. Intentional breaches will result in termination of appointment, and repeated unintentional breaches may result in termination.
   iii. This policy is still binding even after the termination of employment or separation.

3 Logging Management Policy

3.1 Purpose and Scope

a) This logging management and review policy defines specified conditions for information systems to generate, process, aggregate, and store appropriate audit logs across the organization's entire environment to provide critical information and identify indicators of potential compromise.
b) This policy is applicable to every information system within the organization's productivity network.
c) This policy is applicable to every employee, contractor, and partner that administers or renders maintenance on the organization's productivity systems. Within this policy, these individuals are referred to as system administrators.

3.2 The Policy

a) All production systems in the organization shall record and retain audit-logging data that covers the following information:
    i. Activities carried out on the system.
    ii. The user/operator or entity (i.e., system account) that performed the activity, including the system from which the action was performed.
    iii. The file, application, or other objects that the activity was conducted on.
    iv. The time that the activity took place.
    v. The tool used to perform that activity.
    vi. The results of the activity (e.g., success or failure).

b) Particular activities/occurrences to be logged must comprise, at a minimum:
    i. Information (authentication information such as usernames or passwords) created, read, modified, or deleted.
    ii. Accepted or initiated network connections.
    iii. User's authentication and authorization to systems and networks.
    iv. Granting, modifying, or revocating access privileges, including adding new users or groups; changing user privileges, file permissions, database object authorizations, firewall rules, and passwords.
    v. System, network, or services configuration modifications, including software installation, patches application, updates, or other installed software changes.
    vi. Startup, shutdown, or restart of an application.
    vii. Application process abort, failure, or abnormal end, mainly due to resource depletion or stretching a resource to its limit or threshold (such as CPU, memory, network connections, internet bandwidth, disk space, or other resources), the breakdown of network services such as DHCP or DNS, or hardware failure.
    viii. Detection of suspicious and/or malicious activities from a security system such as an Intrusion Detection or Prevention System (IDS/IPS), anti-virus programs, or anti-spyware programs.

c) Unless technically impracticable or infeasible, all logs must be aggregated in a centralized system to correlate, analyze, and track for similarities, trends, and cascading effects across different systems. Log aggregation systems must possess automatic and timely log intake, event and anomaly tagging and alerting, and the ability for manual review.

d) Logs must be manually reviewed regularly:

i. The activities of system users, administrators, and operators must be reviewed on at least a monthly basis.
ii. Logs related to Personal Identifiable Information (PII) must be reviewed on at least a monthly basis to help identify unconventional behavior.

e) When utilizing an outsourced cloud platform, logs must be kept on: the cloud platform's access and uses, resource allocation and utilization, and changes to PII. Logs should be kept for all administrators and operators performing activities in cloud environments.

f) All information systems in the company must synchronize their clocks by executing Network Time Protocol (NTP) or a similar capacity. All information systems must synchronize using the same primary time source.

4 Physical Office Security Policy

4.1 Purpose and Scope

a) This policy institutes the rules governing controls, monitoring, and removal of physical access to the company's facilities.
b) This policy is applicable to every staff, contractor, or third party who requires access to any physical location owned, run, or otherwise occupied by Aya Data Ltd.

4.2 The Policy

a) *Management responsibilities*:
Management shall ensure the provision of the following, but is not limited to:
i. A standard building with office space to accommodate and house personnel and equipment to facilitate a smooth working environment per the business objectives, laws, and regulations as best international practices.
ii. Security areas in layers by designating different security zones within the building. Security zones must include:
1. **Public** - This covers areas of the building or office that are meant for public access.
- Access Restrictions: None
- Additional Security Controls: None
- Examples: Reception, Lobby, common areas of the building
2. **Private -** This includes areas of the building or office used only by employees and other persons for official Aya Data business.
- Access Restrictions: Only Aya Data personnel and approved/escorted guests
- Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, ensuring that any physical access controls are auditable.
- Examples: Hallways, private offices, work areas, conference rooms.
3. **Special Access** - This includes areas restricted to use by certain persons within Aya Data, such as executives, and IT personnel, for security or safety reasons.
- Access Restrictions: Only specifically approved personnel

- Additional Security Controls: Additional access controls must be used, such as keys, keypads, keycards, or similar devices, ensuring that any physical access controls are auditable.
- Examples: Executive offices, lab space, network room, production area, financial offices, and storage areas.

iii. Security personnel on-site.
iv. CCTV
v. Access control mechanisms
vi. Issue all employees photo identification cards

b) *General*:

i. A record of employees with authorized access to the facility shall be maintained with appropriate authorization credentials. The access list and authorization credentials shall be reviewed and approved by authorized personnel periodically.

ii. Information processing offices handling confidential information must be strategically located to minimize the risk of information being exposed to unauthorized persons during their use.
iii. Controls must be adopted to minimize the risk of potential physical and environmental threats.
iv. Equipment must be safeguarded from power failures and other disruptions caused by losses in utilities.

c) *Key access & card systems*:

i. Human Resources maintains a list of authorized key holders approved by management.
ii. Access cards and/or keys must not be given out or borrowed to others.
iii. Access cards and/or keys that users no more require must be returned to Human Resources. Cards must not be reallocated to other individuals, neglecting the return process.
iv. Lost or stolen access cards and/or keys must be reported to Human Resources as soon as realized.
v. In consultation with management, Human Resources must remove the card and/or key access rights of individuals that change roles within Aya Data or are separated from their relationship with Aya Data.
vi. Management must periodically review card and/or key access rights for the facility and remove access for individuals who no longer require access.

c) *Staff & contractor access procedure*:

i. Access to physical locations is given to employees and contractors depending on individual job descriptions and provided by Human Resources.
ii. Any individual granted access to physical spaces would be provided a physical key or access key card. Keys and/or cards issuance is tracked by Human Resources and will be regularly reviewed.
iii. If there is no automated system to log key movements, a record book should be kept to track key holders' in/out activities.
iv. In the case of termination or separation, Human Resources must ensure immediate access revocation (i.e., collection of keys and/or access cards and any other asset used to enter facilities) during the off-boarding procedure.

d) *Visitor & guest access procedure*:

i. Visitors must be given only the level of access to Aya Data premises that is appropriate to the reason for their visit.
ii. Use of visitor access records (sign-in register) shall be maintained.
iii. Designated personnel shall escort visitors, and their activities, if required, shall be monitored.

e) *Audit controls & management*:
Documented procedures and evidence of practice must be in place for this policy.

f) *Enforcement*:
Employees, contractors, or third parties found in breach of this policy (whether intentional or unintentional) may be subject to disciplinary action determined by Aya Data management.

5 Data Retention Policy

5.1 Purpose and Scope

a) The data retention policy establishes the objectives and requirements for data retention within the organization.
b) This policy includes all data within the organization's custody or control, regardless of the medium the data is stored on(i.e., electronic form, paper form, etc.) Within this policy, the medium that holds data is referred to as information, no matter its form.
c) This policy pertains to all users of information systems within the organization. This usually involves employees, contractors, and any external parties that contact systems and information the company owns or manages (hereinafter referred to as "users"). This policy shall be made readily available to all users.

5.2 Background

a) The organization is bound by several legal, regulatory, and contractual commitments concerning the data it retains. These commitments specify the duration data can be retained and how data must be destroyed. Examples of legal, regulatory, and contractual commitments include laws and regulations in the local jurisdiction where the organization conducts business and contracts with employees, customers, service providers, partners, and others.
b) The organization may also be involved in litigation or disaster recovery scenarios requiring it to have access to original information to protect its interests or those of its employees, clients, vendors, partners, and others. Consequently, the organization may need to archive and save information for longer than it may be required for day-to-day operations.

5.3 The Policy

a) *Information Retention*:
i. Retention is defined as the maintenance of information within a production or live environment which an authorized user can access in the ordinary course of business.
ii. Information utilized in the development, staging, and testing of systems must not be retained past their active usage period nor copied into production or live environments.

iii. By default, the information retention period shall be an active use period of precisely two years from its creation, except an exemption is acquired sanctioning a longer or shorter retention period. The business unit accountable for the information must request the exemption.
iv. Information must be archived for a fixed period after the active use of information is ended as per this policy and approved exemption. Once the fixed archive period is ended, the information must be destroyed.
v. Each business unit is accountable for the information it generates, uses, stores, processes, and destroys, according to the requirements of this policy. The accountable business unit is considered to be the information owner.
vi. The organization's legal team may issue a litigation hold to demand that information relating to possible or real litigation, arbitration, or other claims, demands, disputes, or regulatory action be retained as per directions from the legal team.
vii. Every employee and contractor associated with the organization must return information in their ownership or control to the company upon separation and/or retirement.
viii. Information owners must enforce information retention, archiving, and destruction and communicate these periods to relevant parties.

b) *Information Archiving*:

i. Archiving is defined as protected storage of information in a way that the information is rendered unobtainable by authorized users in the regular course of business but can be retrieved by an administrator designated by the organization management.
ii. The default archiving duration of information shall be seven years unless an approved exemption permits a longer or shorter period. The information owner must request for any exceptions.
iii. Information shall be destroyed (defined below) at the end of the elapsed archiving period.

c) *Information Destruction*:

i. Destruction is defined as the technical or physical annihilation to render the information contained in the document permanently irretrievable utilizing ordinary commercially available means.
ii. The organization must enforce and maintain a detailed list of approved destruction techniques suitable for each type of information archived, be it on physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives, or within database files or backup files. Physical information in paper form shall be shredded utilizing an authorized shredding device; waste needs to be periodically removed by approved personnel.

d) *Data Owner's Rights*:

The entities this policy applies to can require us in writing to:

i. Rectify inaccurate information
ii. Stop processing or destroy information that is no longer necessary for processing.
iii. Stop processing or destroy information if your interests override our legitimate grounds for processing the information (whereby we rely on our legitimate interests as a basis for processing information)

iv. Stop processing information for a duration if data is inaccurate or if there is a dispute on whether or not your interests outweigh the Employer's legitimate grounds for processing the information.

e) Retention and archival periods for information collected, created, processed, stored, and used by the organization are defined internally according to legal, regulatory, and contractual obligations.

6 Risk Assessment Policy

6.1 Purpose and Scope

a) This policy aims to define the approach for assessing and treating information security risks across the organization and determining the acceptable level of risk (tolerance) set by the organization's leadership.
b) Risk assessment and risk treatment are applicable to the entire scope of the organization's information security program and to all assets used within the organization or which could impact information security within it.
c) This policy is applicable to all employees of the organization who take part in risk assessment and risk treatment.

6.2 Background

A vital part of the organization's information security program is a comprehensive and systematic approach to risk management. This policy defines the requirements and procedures for the organization to determine information security risks. The process is made up of four parts: identification of the organization's assets, along with the threats and vulnerabilities that apply; evaluation of the likelihood and consequence (risk) of the threats and vulnerabilities being recognized; identification of treatment for each intolerable risk; and evaluation of the residual risk after treatment.

6.3 The Policy

a) *Risk Assessment*:
   i. The risk assessment method involves the identification of threats and vulnerabilities associated with company assets.
   ii. Firstly, the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets that may impair the confidentiality, integrity, and/or availability of information in the organization. Assets may comprise documents in paper or electronic form, applications, databases, information technology facilities, infrastructure, and external/outsourced services and processes. For every asset, an owner shall be identified.
   iii. The next is to identify all threats and vulnerabilities affiliated with each asset. Threats and vulnerabilities shall be listed in a risk assessment table where an asset may be linked with multiple threats, and each threat may be linked to numerous vulnerabilities. A risk assessment table is provided as part of the Risk Assessment Report Template (reference (Table 1&2:)).
   iv. For every risk, an owner shall be identified. The risk owner and the asset owner could be the same person.
   v. Once risk owners are determined, they must assess.

vi. The risk level is measured by adding the impact (consequence) score and the likelihood score.

Table 1: Description of Consequence Levels and Criteria:

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event would be anticipated to have **various severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be anticipated to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic negative impact means that, for example, the threat event might: (i) cause severe deterioration in or loss of mission capacity to an extent and duration that the organization is unable to discharge one or more of its principal functions; (ii) result in substantial damage to organizational assets; (iii) result in substantial financial loss; or (iv) result in severe or catastrophic damage to individuals including loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be anticipated to have a **se**vere negative effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe adverse effect means that, for example, the threat event might: (i) cause substantial deterioration in mission capacity to an extent and duration that the organization can discharge its principal functions, but the effectiveness of the functions is substantially reduced; (ii) result in substantial damage to organizational assets; (iii) result in substantial financial loss; or (iv) result in substantial harm to individuals but not involving loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be anticipated to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A limited negative impact means that, for example, the threat event might: (i) cause deterioration in mission capacity to an extent and duration that the organization can discharge its principal functions, but the effectiveness of the functions is noticeably decreased; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be anticipated to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 2: Description of Likelihood Levels and Criteria:

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	An adversary is **almost certain** to initiate the threat event.
High	80-95	8	An adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	An adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	An adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	An adversary is **highly unlikely** to initiate the threat event

b) *Risk Assessment*:
   i. Risk values 0 through 20 are considered to be acceptable risks
   ii. Risk values 21 and 100 are considered to be unacceptable risks. Unacceptable risks must be treated

c) *Risk Treatment*
   i. Risk treatment is executed through the Risk Treatment Table. Every risk from the Risk Assessment Table must be transferred to the Risk Treatment Table for disposition, together with treatment choices and residual risk.
   ii. As part of the risk treatment process, the CEO and/or other company managers shall establish objectives for alleviating or treating risks. All unacceptable (intolerable) risks must be treated. For constant improvement purposes, organization managers may also opt to treat other risks for company assets, even if their risk score is considered to be acceptable.
   iii. After choosing a treatment option, the risk owner must estimate the new consequence and likelihood values after implementing the planned controls.

d) *Regular Reviews of Risk Assessment and Risk Treatment*
   i. The Risk Assessment Table and Risk Treatment Table must be reviewed and updated when new risks are identified. At a minimum, this review and update shall be conducted once per year. The Risk Assessment and Risk Treatment Table is highly recommended to be reviewed and updated when substantial modifications happen in the organization, its technology, business objectives, or business environment.

e) *Reporting*
   i. The risk assessment and treatment results, and all subsequent reviews, shall be documented in a Risk Assessment Report.

7 Data Anonymisation and Pseudonymisation Policy

7.1 Purpose and Scope

a) This policy aims to ensure a standardized approach to warrant consistency throughout Aya Data concerning how and when to anonymize or pseudonymize information correctly. This policy should be read alongside the complete set of Aya Data's Data Protection policies, particularly the confidentiality policy, to ensure guidance and

safeguard confidentiality when the data is used for purposes other than the primary intended use.

b) This policy is applicable to every full-time employee, part-time employee, and contractor who receives, controls or processes personal data during their engagement period;
c) Third-party companies (data processors) that receive, handle, or process personal data on behalf of Aya Data;
d) All must comply with this policy where anonymized and pseudonymized information is produced or shared from individual-level data;
e) Adherence to applicable policies is binding under their Employment Offer Letter and/or Independent Contractor Agreement.

7.2 Background

Continuous compliance with the General Data Protection Regulation (GDPR) 2018 requires Aya Data to use the minimum personal data necessary for any particular purpose. Secondary usage of private information must not breach our responsibilities of confidentiality and respect for private and natural life. This guidance identifies how we use anonymization and pseudonymization to remove identifiable information relating to individuals' data. Anonymization and pseudonymization enable Aya Data to undertake secondary use of personal data safely, securely, and legally.

7.3 Definitions

Anonymisation and pseudonymization both relate to the concealment of an individual's identity.

a) **Anonymisation** is the technique of eliminating, substituting, and/or altering any identifiable information (identifiers) that can point to the person(s) it pertains to, thereby irreversibly preventing the identification of the individual to whom it relates. Data can be considered effectively and adequately anonymized if it does not connect to an identified or identifiable natural person(s) or where it has been rendered anonymous such that the data subject is not or no more identifiable.
b) **Pseudonymisation** is the technical method of substituting any identifying attributes of data with a pseudonym or a value that does not permit the data subject to be directly identified, thus protecting the individual's identity. Supposing the same system of pseudonyms is applied across different datasets, these datasets can be merged for analytical objectives without exposing the identities of individuals. Caution needs to be taken if merging datasets, as this could lead to individuals being identifiable via a combination of their circumstances. Substituting an original name with a nickname is an example of pseudonymization; nonetheless, other identifying information like age, ethnicity, gender, or particular medical status may also be substituted to protect the individual’s identity.
c) **Aggregation** is an anonymization procedure in which information is only given as totals so that no information identifying individuals is presented. Low numbers presented in total are a risk and may need to be omitted or 'blurred' utilizing random addition and subtraction.
d) **Personal Identifiable Information (PII)** is any information that can directly identify an individual. This could be a single piece of information, or a combination of information, for example, a name, unique reference number, and date of birth.
e) **Primary use** represents the use of information for the purpose of delivering Aya Data services to clients. This also comprises relevant supporting administrative procedures and audit/assurance of the quality of services offered. Primary usage requires information at the person identifiable level (example, Name, Address, Date of Birth, Postcode, NHS/NHIS number, Ethnic category, Unique booking reference number, social security number, etc.).

f) **Secondary use** represents the use of information about individuals for data labelling, machine learning, research, audits, service management, commissioning, contract monitoring, and reporting purposes. When PII is utilized for secondary uses, the identifiable information must be limited and de-identified such that the secondary use operation does not permit individuals to be identified.

g) **Re-identification or de-anonymization** is where anonymized information is turned back into personal information through the use of, for example, data matching or combining. Where anonymization is being undertaken, the process must be designed to minimize the risk of re-identification.

7.4 The Policy

a) **Anonymization**:

i. Staff must only possess access to the information that is essential for the completion of the business operations they are engaged in. This principle pertains to the use of PII for secondary or non-direct objectives. Employing de-identification equips users to make use of individual information for a variety of secondary purposes without accessing identifiable information items.

ii. De-identification or anonymization aims to adequately conceal the identifiable information items embedded in the person's records. The risk of possible identification of the information subject is minimized to acceptable levels; this will provide adequate anonymization.

iii. De-identification can be accomplished via a variety of methods. De-identification accomplishment depends on the appropriateness of the technique applied to a specific dataset. Methods comprise:

- Aggregation, such that information is solely seen as totals.
- Eliminating personal identifiers.
- Utilizing identifier ranges, for example: age ranges instead of exact age, partial postcode or super output area rather than the full address, age at activity event instead of the date of birth.

iv. De-identified information that descends to the individual level should still be used within a secure environment, employing staff access control to data as an example.

b) **Pseudonymization:**

i. When pseudonymization techniques are consistently applied, the same pseudonym is provided for individuals across different datasets. Over time, this enables datasets and other information to be linked in ways that would be impossible if personally identifiable information was eliminated.

ii. To effectively pseudonymize information, the following actions are to be taken:

- Every PII field must have a unique pseudonym;
- Pseudonyms to be utilized in place of unique identification numbers (example: NHS/NHIS number) and related fields should be of equal length and formatted on output to warrant readability. For instance, to replace NHS/NHIS numbers in existing report formats, the outputted pseudonym must have equal field length but not the same characters.
- Other identifiable fields must be substituted by alternatives that render the information less deducible (e.g., age at activity event substituting date of birth, lower super output area replacing postcode).

- It should be evident from the format of pseudonym information that it is not 'original' information to prevent confusion, e.g., adding letters that would not generally be part of NHS/NHIS numbers.
- Where used for external purposes, pseudonyms usage must give different pseudonym values so that internal pseudonyms are not exposed;
- where pseudonyms are employed for secondary use, the output must only display the pseudonymized data items that are required;
- Pseudonymized information should have the same security as PII.

c) Exceptions.
   i. In the event, records are utilized in an identifiable manner for purposes other than regular service delivered by Aya Data. In that case, the reasons and usage of the information should be fully documented and approved by the appropriate information owner and Aya Data management.
   ii. Appropriate personnel should set up the proper tracking tool to document this activity, e.g., an Excel spreadsheet. The essential items to be reported are:
      - Who has accessed each database containing identifiable information;
      - Date and time of access;
      - The reason for the access;
      - The output from the access.
   iii. A structured log of accesses should be kept to enable queries and audits. The record of accesses must be regularly audited to check for unusual patterns of access.

d) Awareness and Training.
   i. Appropriate training on the implementation and use of anonymized and pseudonymized information/data shall be provided by Aya Data as required.
   ii. All staff is required to undertake mandatory policies training per the Policy training Policy of Aya Data. More specialist training and support are also available as deemed appropriate by the management of Aya Data.