SERVICE PROVIDER MINIMUM SECURITY CONTROL REQUIREMENTS

This document describes the Minimum Security Control Requirements ("**Minimum Control Requirements**") that Service Providers engaged or proposed to be engaged by Alnylam Pharmaceuticals, Inc. and its affiliates (hereinafter "Alnylam") are required to adhere to in the provision of the agreed Services, especially to the extent that personal data (as defined in applicable data protection laws and regulations, including but not limited to the EU General Data Protection Regulation (hereinafter "GDPR")) are to be subjected to any and all kinds of processing operations by such Service Providers acting for and on behalf of Alnylam, and under its documented instructions.

These Minimum Control Requirements are stated at a relatively high level. Alnylam recognizes that there may be multiple acceptable approaches to accomplish a particular Minimum Control Requirement. Service Provider must document in reasonable detail how a particular control meets the stated Minimum Control Requirement. This document includes only an indicative list of the proposed measures to be implemented in practice by engaged Service Providers; , however, depending on the nature or scope of the Services to be provided, the actual implemented controls may vary among Service Providers and also among Services. Service Provider shall review regularly and at a minimum once every year, and if necessary revise the Minimum Control Requirements to ensure that they are still deemed adequate with regard to ensuring an appropriate level of security of the Personal Data Processed.

The term "should" in these Minimum Control Requirements means that Service Provider will use commercially reasonable efforts to accomplish the stated Minimum Control Requirement, and will document those efforts in reasonable detail, including the rationale, for any deviations.

As used in these Minimum Control Requirements, (i) "**including**" and its derivatives mean "including but not limited to"; (ii) any capitalized terms not defined herein shall have the same meaning as set forth in the Master Contract Services Agreement executed in writing between Alnylam and such Service Provider relating to the Services to be provided to Alnylam to which these Minimum Control Requirements relate (the "**Agreement**").

PART A DEFINITIONS

1. "**Systems**" means Service Provider's information systems.
2. "**Assets"** means Service Provider's information assets (e.g., data).
3. "**Facilities"** means Service Provider's facilities, whether owned or leased by Service Provider (e.g., AWS, data centers).
4. "**Dependent suppliers**" means Service Provider's key vendors/suppliers.

PART B TECHNICAL AND ORGANIZATIONAL MEASURES

I. ESSENTIAL ELEMENTS TO ENSURE THE TARGETED LEVEL OF SECURITY

1. RISK MANAGEMENT

Risk Management Strategy & Program. Governance and Risk Management strategy and assessment program are established and maintained to manage internal and external threats. Risk strategy should be documented based on the results of risk assessments, a risk register should be kept up to date, and corresponding risk treatment plans are established to manage risk to an appropriate level to protect data. The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.

Risk and Impact Assessments. A risk assessment must be performed annually to verify the implementation of controls that protect business operations and Confidential Information. Impact assessments are regularly performed in accordance with applicable laws and regulations. Risks identified in impact assessments are appropriately documented and triaged in accordance with the risk register and risk treatment plan.

2. ENCRYPTION

Encryption. Cryptographic protections are employed to preserve the confidentiality and integrity of sensitive data when it is processed, stored, or transmitted, including when shared with dependent suppliers.

Encryption Policies, Procedures, and Practices. Policies, procedures, and practices covering the use and application of encryption are documented, reviewed, approved and communicated.

Encryption Requirements. Alnylam Confidential data must be encrypted in accordance with minimum baseline encryption standards while in transit and at rest.

Encryption Uses.

- Confidential Information must be protected, and should be encrypted when stored and while in transit over any network.
- Authentication credentials must be encrypted at all times, in transit or in storage.
- Removable media containing Confidential Information must be encrypted.
- Applications and databases containing sensitive data are encrypted based on a risk assessment.
- Full-disk encryption is used to encrypt workstations and laptops that contain sensitive data.
- Sensitive data in transit is encrypted using secure communication protocols

- Encryption keys are generated using approved key management solution with minimum key complexity requirements.

- Access to encryption keys is restricted and a process to change encryption keys is established (e.g., expiration, termination of individual with knowledge of keys).

3. PSEUDONYMIZATION

If personal data cannot be anonymized or minimized due to processing requirements, it should be pseudonymized so the data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

Pseudonymization. Pseudonymized data should be used when real data is not required or presents additional risk to the organization. If data can be anonymized and used for the same purposes, then anonymization should be used instead of pseudonymized data.

- Access to information used to reverse data de-identification (e.g., linking identifiers to identify sensitive data) must be limited to appropriate personnel.

- Reversal of de-identification must follow a documented process and require approval.

- Capabilities are in place to de-identify or remove personal data used for testing purposes

II. REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY INTEGRITY AVAILABILITY AND RESILIANCE OF PROCESSING SYSTEMS AND SERVICES

Requirements for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services are covered throughout the Operations, Integrity, and Encryption sections, as well as below.

1. DATA INTEGRITY

Controls must ensure that any data stored, received, controlled or otherwise accessed is accurate and reliable. Procedures must be in place to validate data integrity throughout the data life cycle, including in the creation, modification, processing, maintenance, archival, retrieval, transmission, and disposition of data after the record's retention period ends.

- **Data Quality Controls**. Sensitive data collected, stored and processed is subject to data quality checks to ensure completeness, accuracy and relevancy.

- **Data Transmission Controls.** Processes, procedures and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, to ensure data integrity during transmission and to validate that the data transmitted is the same as data received.

- **Data Transaction Controls.** Controls must be in place to protect the integrity of data transactions at rest and in transit.

- **Data Storage Controls.** Sensitive data is stored in approved data repositories in accordance with applicable statutory, regulatory and/or contractual obligations.

- **Data Policies.** A policy must be in place to cover data classifications, encryption use, key and certificate lifecycle management, cryptographic algorithms and associated key lengths. This policy must be documented, reviewed, and approved with management oversight, on a periodic basis.

- **Backup and Recovery Procedures.** Backup data and copies of data should be validated for accuracy, completeness and secure from alteration, inadvertent erasures, or loss.

III. REQUIREMENTS FOR THE ABILITY TO RESTORE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

Requirements for the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident are described throughout Business Continuity and Disaster Recovery, and Incident Response sections, as well as below.

1. ADDITIONAL REQUIREMENTS FOR THE USE OF CLOUD TECHNOLOGY

Adequate safeguards must ensure the confidentiality, integrity, and availability of Alnylam Data stored, processed or transmitted using cloud technology (either as a cloud Alnylam or cloud provider, to include dependent suppliers), using industry standards. Cloud management controls are implemented to ensure cloud instances are secure and in line with industry practices.

- **Audit Assurance and Compliance.** The cloud environment in which data is stored, processed or transmitted must be compliant with relevant industry standards and regulatory restrictions.

- **Vendor selection.** Service Provider must have a process to evaluate Cloud vendors providing hosting or support services to Service Provider prior to selection. Third-party service providers must demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.

- **Subnet management.** Secured and encrypted communication channels are used when migrating physical servers,

applications, or data to virtualized servers and use a network segregated from production-level networks for such migrations.

- **Interoperability.** Multi-tenant owned or managed assets (physical and virtual) are designed and governed so that provider and customer (tenant) user access is appropriately segmented from other tenant users.

- **Application and Interface Security.** Threat modeling should be conducted throughout the software development lifecycle, including vulnerability assessments, including Static/Dynamic scanning and code review, to identify defects and complete remediations before hosting in cloud environments.

- **Business Continuity Management and Operational Resiliency**. Business continuity plans to meet recovery time objectives (RTO) and recovery point objectives (RPO) must be in place.

- **Data Security and Information Lifecycle Management.** Proper segmentation of data environments and segregation must be employed; segmentation/segregation must enable proper sanitization, per industry requirements.

- **Encryption and Key Management.** All communications must be encrypted in transit and at rest between environments.

- **Governance and Risk Management.** Comprehensive risk assessment processes and centralized monitoring that enables incident response and forensic investigation must be used to ensure proper governance and oversight.

- **Identity and Access Management.** Management of accounts, including accounts with privileged access, must prevent unauthorized access and mitigate the impacts thereof.

- **Infrastructure and Virtualization Security.** Controls defending against cyberattacks, including the principle of least privilege, baseline management, intrusion detection, host/network-based firewalls, segmentation, isolation, perimeter security, access management, detailed data flow information, network, time, and a SIEM solution must be implemented.

- **Supply Chain Management, Transparency and Accountability.** Service Provider must be accountable for the confidentiality, availability and integrity of production data, to include data processed in cloud environments by dependent suppliers.

- **Threat and Vulnerability Management.** Vulnerability scans (authenticated and unauthenticated) must be performed, both internally and externally, for production systems. Processes must be in place to ensure tracking and remediation.

2. INCIDENT RESPONSE

A documented plan and associated procedures, to include the responsibilities of Service Provider personnel and identification of parties to be notified in case of an information security incident, must be in place.

Incident Response Process. The information security incident management program must be documented, tested, updated as needed, reviewed, and approved, with management oversight, on a periodic basis. The incident management policy and procedures must include prioritization, roles and responsibilities, procedures for escalation (internal) and notification, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity. A root cause analysis is performed to identify where corrective controls and preventive measures should be taken in the future.

Data breach response – Incident response procedures must include a comprehensive model to respond to and mitigate breaches of personal data to meet regulatory and Agreement requirements.

3. BUSINESS CONTINUITY AND DISASTER RECOVERY

Service Provider must have formal documented recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable.

- **Business Recovery Plans**. Comprehensive business resiliency plans addressing business interruptions of key resources supporting services, including those provided by dependent suppliers, must be documented, tested, reviewed, and approved, with management oversight, on a periodic basis. The business resiliency plan must have an acceptable alternative work location in place to ensure service level commitments are met.

- **Technology Recovery.** Technology recovery plans to minimize service interruptions and ensure recovery of systems, infrastructure, databases, applications, etc. must be documented, tested, reviewed, and approved with management oversight, on a periodic basis.

- **Back-ups**. Service Provider must have policies and procedures for back-ups of Alnylam Data. Back-ups must be protected using industry best practices and tested for integrity. Access should be limited based on need and processing requirements. Retention periods should align with company policies and processing requirements.

- **Remediation and response**. Contingency plans/business recovery plans are initiated in a timely manner in response to incidents. **Back-up and Redundancy Processes.** Processes enabling full restoration of production systems, applications, and data must be documented, reviewed, and approved, with management oversight, on a periodic basis.

4. PHYSICAL AND ENVIRONMENTAL

Controls must be in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.

- **Physical and Environmental Security Policy.** Physical and environmental security plans must exist for facilities and scenarios involving access or storage of Alnylam Data. Additional physical and environmental controls must be required and enforced for applicable facilities, including servers and datacenter locations. Policies must be in place to ensure that information is accessed on a controlled and need-to-know basis.
- **Physical Control.** Storage of Alnylam Data at new facilities or locations that are not a Service Provider facility, as defined herein, must be pre-approved by Alnylam before use.
- **Physical Access to Facilities** - Facilities where information systems that process Alnylam Data must be restricted to authorized personnel, including visitors and temporary employees. All access periodically reviewed. Terminated user access is removed in a timely manner.
- **Physical Access to Components.** An accurate record of incoming and outgoing media containing Alnylam Data, including the kind of media, the authorized sender/recipients, data and time, the number of media and the types of data they contain.
- **Environmental Control.** Facilities, including data and processing centers, must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection. Environmental control components must be monitored and periodically tested.
- **Protection from disruptions.** Industry standard systems should be used to protect against loss of data due to power supply failure or line interference. **Component disposal.** Industry standard processes must be used to delete or remove Alnylam Data when it is no longer needed.
- **Safe Travel Protocols.** Appropriate protocols are applied to protect personal data in the event employees or contractors are travelling outside designated home and office locations for business purposes.

IV. REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSRURING THE SECURITY OF THE PROCESSING

Requirements for processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing discussed throughout Organizational Security, Encryption, and Operations sections, as well as below.

1. VULNERABILITY MONITORING

Service Provider must continuously gather information and analyze vulnerabilities in light of existing and emerging threats and actual attacks. Processes must include vulnerability scans, anti-malware, Intrusion Detection Systems (IDS)/Intrusion

Prevention Systems (IPS), logging and security information and event management analysis and correlation.

- **Vulnerability Scanning and Issue Resolution.** Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically and prior to system provisioning for production systems that process, store or transmit Alnylam Data. All applications, systems, and components are subject to authenticated vulnerability scanning unless there is an approved, documented exception.

- **Malware.** In production, Service Provider must employ tools to detect, log and disposition malware.

- **Intrusion Detection/Advanced Threat Protection.** Network and host-based intrusion detection/advanced threat protection must be deployed with events generated fed into centralized systems for analysis. These systems must accommodate routine updates and real-time alerting. IDS/advanced threat protection signatures must be kept up-to-date to respond to threats.

- **Logging and Event Correlation.** Monitoring and logging must support centralization of security events for analysis and correlation. Organizational responsibility for responding to events must be defined. Retention schedule for various logs must be defined and followed.

2. AUDIT

At least annually, Service Provider will conduct an independent third-party review of its security policies, standards, operations and procedures related to the Services provided to Alnylam. Such review will be conducted in accordance with the AICPA's Statements on Standards for Attestation Engagements (SSAE), and Service Provider will be issued a SOC 2 Type II report. Absent a SOC 2 Type II report, Alnylam will also accept a third-party expert compliance report or self-attestation of compliance. Upon Alnylam's request, Service Provider will provide Alnylam with a copy of the report within thirty (30) days. If applicable, Service Provider will provide a bridge letter to cover time frames not covered by the audit period scope within 30 days, upon request by Alnylam. If exceptions are noted in the audit, Service Provider will document a plan to promptly address such exceptions and shall implement corrective measures within a reasonable and specific period. Upon Alnylam's reasonable request, Service Provider will keep Alnylam informed of progress and completion of corrective measures.

- Alnylam shall rely on the third-party audit report for validation of proper information security practices, and will not proceed to additional audits, except if not satisfied with the contents of the report provided by the Service Provider or in the case of a Security Breach resulting in a Personal Data Breach or in a material business impact to Alnylam.
- If Alnylam exercises the right to audit as a result of a Security Breach and/or Personal Data Breach, such audit shall be within the scope of the Services. Alnylam will provide Service Provider a minimum of thirty (30) days of notice prior to such onsite audit. Service Provider shall have the right to approve any third-party Alnylam may choose to fully conduct on its behalf or be involved in the audit.

V. REQUIREMENTS FOR USERS INDENTIFICATION AND AUTHORISATION

Requirements for user identification and authorization discussed throughout Physical and Environmental sections, as well as below.

1. ACCESS CONTROL

Authentication systems must be configured to enforce authentication requirements and secure logon procedures. Authorization systems enforce approved authorizations for access to information and system resources, and user access to system functionality and data is restricted based on approved access privileges and authorizations. Authorization controls must be appropriate for the risk of the system, data, application and platform; access rights must be granted based on the principle of least privilege, align to classification of the data based on risk, and monitored to log access and security events, using tools that enable rapid analysis of user activities.

- **Logical Access Control Policy.** Documented logical access policies and procedures must support role-based, "need-to-know" access, timely de-provisioning of access upon termination, transfer, or determination of inappropriate access, and ensure separation of duties during the approval and provisioning process. Each account provisioned must be uniquely identified and account holders are informed of acceptable use standards and access control policies at the time of account provisioning. User access reviews must be conducted at least annually to evaluate appropriateness of access.
- **Privileged Access.** Provisioning of privileged user accounts (*e.g.*, those accounts that have the ability to override system controls), to include service accounts, must follow a documented process and be restricted. A periodic review and governance process must be performed at least quarterly to ensure appropriateness of privileged access is maintained.
- **Authentication and Authorization**. A documented authentication and authorization policy must cover all applicable systems. That policy must include strong authentication requirements, including but not limited to, password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized. Authentication credentials must be encrypted, including in transit to and from dependent suppliers' environments or when stored by dependent suppliers.

VI. REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION

The requirements for the protection of data during transmission are discussed throughout the Encryption section, as well as below.

1. COMMUNICATION AND CONNECTIVITY

Service Provider must implement controls over its communication network to safeguard data. Controls must include securing the production network and implementation of encryption, logging and monitoring, and disabling communications

where no business need exists.

- **Network Identification.** A production network diagram, to include production devices, must be kept current to facilitate analysis and incident response.
- **Data Flow Mapping**. A current data flow diagram must depict data relevant to the Agreement from origination to endpoint (including data which may be shared with dependent suppliers).
- **Data Storage.** All Alnylam Data, including Alnylam Data shared with dependent suppliers, must be stored and maintained in a manner that allows for its return or secure destruction upon request from Alnylam.
- **Firewalls & Firewall Management.** Firewalls must be used for the isolation of all environments, to include physical, virtual, network devices, production and non-production, and application/presentation layers. Firewall management must follow a process that includes restriction of administrative access and that is documented, reviewed, and approved, with management oversight, on a periodic basis. The production network must be either firewalled or physically isolated from any development and test environments. Multi-tier security architectures that segment application tiers (*e.g.*, presentation layer, application and data) must be used.
- Periodic network vulnerability scans must be performed and any critical vulnerabilities identified must be remediated within a defined and reasonable timeframe.
- **Remote Access.** The data flow in the remote connection must be encrypted and multi- factor authentication must be utilized during the login process. Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (*i.e.*, no split tunneling). Dependent suppliers' remote access, if any, must adhere to the same controls and must have a valid business justification.
- **Wireless Access.** Wireless access to the Service Provider corporate network must be configured to require authentication and be encrypted.

VII. REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE

Data storage. Policies and procedures are documented, reviewed, approved, and communicated, which cover secure data storage protocols. Information assets containing sensitive data are contained in approved and secure data zones in accordance with applicable statutory, regulatory, and/or contractual obligations.

- New data repositories required for the processing of sensitive data are requested, reviewed, approved, and tracked.

- A data catalog is documented and maintained to profile sensitive data assets across the organization

- Testing is performed on a periodic basis to validate that data is segmented in accordance with applicable data localization and data residency requirements.

- Sensitive data is securely disposed when no longer required for a business, contractual, legal or regulatory

purpose.

VIII. REQUIREMENTS FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED

Requirements for physical security of locations at which Personal Data are processed are discussed throughout Physical and Environmental section.

IX. REQUIREMENTS FOR EVENTS LOGGING

Event logging. Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach. Capabilities and processes exist to detect and respond to potential incidents through a formalized intake of security-related tickets, log monitoring, and analyzing threat intelligence feeds to be escalated accordingly.

- **Log generation.** All systems that contain sensitive data must generate logs that contain sufficient data to detect anomalous or suspicious activity and to support forensic capabilities. Logs must be stored securely and write access to audit logs restricted.

- The organization logs all counterfeit or foreign equipment and takes it off the network to be forensically analyzed.

- **Clock Synchronization.** Production network devices must have internal clocks synchronized to reliable time sources.
- **Log Management.** Logs should be forwarded to a centralized location for review and monitoring. Access to centralized audit logs should be restricted to authorized personnel with read-only access.

- Event detection information is communicated to appropriate parties, including Alnylam for high risk incidents or suspected data breaches.

X. REQUIREMENTS FOR SYSTEM CONFIGURATION, INCLUDING DEFAULT CONFIGURATION

Requirements for system configuration, including default configuration, discussed throughout Asset Management section.

XI. REQUIREMENTS FOR INTERNAL IT AND IT SECURITY GOVERNANCE AND

MANAGEMENTS

1. ORGANIZATIONAL SECURITY

A personnel security policy must be in place to establish organizational requirements to ensure proper training, competent performance and an appropriate and accountable security organization.

- **Security Ownership**. Service Provider must appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.
- **Organization**. Current organizational charts representing key management responsibilities for services provided must be maintained.
- **Background Checks.** Where legally permissible, background checks (including criminal) must be performed on applicable Service Provider personnel.
- **Confidentiality Agreements.** Service Provider personnel must be subject to written non-disclosure or confidentiality obligations.
- **Security Awareness Training & Education.** Service Provider informs its personnel about relevant security procedures and their respective roles. Service Provider also informs its personnel of possible consequences of breaching the security rules and procedures. Service Provider personnel must receive security training at least annually and on an ongoing basis, depending upon need and risk to sensitive data.

2. SECURITY POLICY

A documented set of rules and procedures must regulate the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of information and associated services.

- **Security Policy Implementation and Review.** Security policies must be documented, reviewed, and approved, with management oversight, on a periodic basis, following industry best practices.
- **Roles and Responsibilities**. Roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
- **Policy Exception Management.** A risk-based exception management process must be in place for prioritization, approval, and remediation or risk acceptance of controls that have not been adopted or implemented.
- Communication of Policies. Information Security and Privacy policies and procedures are published and communicated to all employees and relevant external parties.

3. TECHNOLOGY ASSET MANAGEMENT

Controls must be in place to protect Service Provider IT and information assets, including mechanisms to maintain an accurate and up-to-date inventory of IT and information assets throughout the asset lifecycle and handling standards for introduction and transfer, removal and disposal of IT and information assets.

- **Asset inventory.** A centralized inventory of organizational IT assets is developed and maintained to capture asset-specific information.
- **Accountability**. A process for maintaining an inventory of hardware and software assets and other information resources, such as databases and file structures, must be documented. Process for periodic asset inventory reviews must be documented. Identification of unauthorized or unsupported hardware/software must be performed.
- **Asset Handling**. Service Provider classifies sensitive data to help identify it and allow for access to it to be appropriately restricted. Personnel must obtain authorization prior to storing sensitive data on portable devices, remotely accessing Alnylam data, or processing Alnylam data outside of Service Provider facilities.
- **Asset Disposal or Reuse**. If applicable, Service Provider will use industry standards to securely delete, anonymize without the ability to re-identify, or carry out physical destruction as the minimum standard for disposing of information assets. Service Provider must have documented procedures for disposal or reuse of information assets. **Data Subject Requests**. Procedures must be in place to remove data and retrieve data for access requests or manage consent requirements, if applicable, from information systems in which Alnylam Data are stored, processed, or transmitted.
- **Default configurations**. Baseline configurations are developed and documented to maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards.
    - Baseline configurations are reviewed and updated. This includes both routinely and as part of system component installations and upgrades.
    - Previous versions of baseline configuration are securely stored and retained to support roll back in the event of a security incident.

4. STANDARD BUILDS

Production systems must be deployed with appropriate security and privacy configurations and reviewed periodically for compliance with Service Provider's security policies and standards.

- **Secure Configuration Availability.** Standard security configurations must be established and security hardening demonstrated. Process documentation must be developed, maintained, and under revision control, with management oversight, on a periodic basis. Configurations must include security patches, vulnerability management, default passwords, registry settings, file directory rights and permissions.
- **System Patches.** Security patch process and procedures, to include requirements for approval and timely patch application, must be documented.
- **Operating System.** Versions of operating systems in use must be supported and respective security baselines documented.
- **Desktop Controls.** Systems must be configured to provide only essential capabilities. The ability to write to removable media must be limited to documented exceptions.
- **Mobile Devices.** Only approved mobile devices (smartphones, laptops, USBs, external hard drives) shall be used to host or access Alnylam Data. USBs and portable hard drives are not to be used for storing Sensitive Personal

Information, unless explicitly approved by Alnylam.

5. CHANGE MANAGEMENT

Changes to the production systems, production network, applications, data files structures, other system components and physical/ environmental changes must be monitored and controlled through a formal change control process. Changes must be reviewed, approved and monitored during post-implementation to ensure that expected changes and their desired result are accurate.

Change Policy and Procedure. A change management policy, including application, operating system, network infrastructure and firewall changes must be documented, reviewed and approved, with management oversight, on a periodic basis.

- The change management policy must include clearly identified roles and responsibilities to support separation of duties (e.g., request, approve, implement). The approval process must include pre- and post-evaluation of change.

Configuration Changes. Mechanisms are in place to validate that controls, configurations, and policies are implemented and continuously operating effectively.

- Configuration, rules, and policy changes are reviewed periodically to determine whether changes in configuration are necessary.
- Where feasible, audit logging is enabled for assets and technologies to monitor and review configuration changes.

6. OPERATIONS

Documented operational procedures must ensure correct and secure operation of Service Provider's assets. Operational procedures must be documented and include monitoring of security events, capacity, performance, service level agreements and key performance indicators.

- **Security Monitoring.** Capabilities exist to monitor for potential threats and compromises. Events are detected and appropriate personnel are notified to respond. Response procedures follow a documented and approved process.
- **Data loss Prevention.** Policy-based capabilities are used to detect, investigate, block, and monitor for loss of data commensurate with its classification to prevent the unauthorized storage, transmission, or usage of data
- **Endpoint configuration.** Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.
- Personal Information, unless explicitly approved by Alnylam.

XII. REQUIREMENTS FOR CERTIFICATION / ASSURANCE OF PROCESSES AND PRODUCTS

- **Compliance with security baseline requirements**. Processes exist to perform privacy impact assessments and security reviews periodically and prior to implementing new or making changes to existing processes or products. Deviations from baselines are monitored by a separate function within the organization and remediated in a timely manner.

- **Security assessments** must be reassessed at least annually and include at a minimum:

    - Technical capabilities are used to prevent the disclosure of sensitive data required for business purposes

    - Review of cross-border transfers of personal data to validate jurisdictions are not restricted

    - Purpose and use of personal data aligns to notice

    - Access to data is limited to appropriate personnel

    - Sensitive data is encrypted

XIII. REQUIREMENTS FOR MINIMISATION, DATA QUALITY, RETENTION AND ACCOUNTABILITY

Service Provider must ensure the personal data processed is:

- Adequate – sufficient to properly fulfil stated purpose

- Relevant – has a rational link to that purpose; and

- Limited to what is necessary – only hold the data needed for that purpose

Data minimization. The collection of personal data is limited to the minimum amount necessary to carry out the specified business purpose.

Data quality. Policies cover the implementation and maintenance of data quality standards throughout the data lifecycle. Instances of inaccurate or incomplete sensitive data identified are remediated.

Data retention. Retention schedules are documented, reviewed, approved, and communicated, which cover the minimum length of time a record or copy needs to be retained before disposal. Data retention rules are applied to information assets and paper records containing sensitive data based on a risk assessment.

Accountability. A Data Protection Officer (DPO) or equivalent role in the executive leadership function within the organization is accountable for the organization's established data protection and privacy compliance and oversight.

Alleged regulatory violations and internal policy violations are reviewed in a timely manner.

XIV. REQUIREMENTS FOR DATA PORTABILITY AND DATA DISPOSAL

Data format. Personal data is stored in a machine-readable format and may be produced within a reasonable time period at the request of the Controller.

Data disposal. Policies are documented, reviewed, approved, and communicated, which cover secure data disposal protocols for information assets and paper records.

- Information assets and paper records containing sensitive data are reviewed on a periodic basis to determine if the data should be retained, de-identified, or deleted in accordance with the organizational retention policy.
- Sensitive data marked for disposal is reviewed and approved prior to disposal action.

XV.THIRD PARTY RELATIONSHIPS

Key dependent suppliers must be identified, assessed, managed and monitored. Dependent suppliers that provide material services, or that support Service Provider's provision of material services to Alnylam, must comply with control requirements no less stringent than those outlined in this document.

- **Selection and Oversight.** Service Provider must have a process to identify key dependent suppliers providing services to Service Provider; these dependent suppliers must be disclosed to Alnylam and approved to the extent required by the Master Contract Services Agreement and/or the Data Processing Agreement. Risk assessments of each dependent supplier's control environment must be performed periodically.
- **Inventory of Third Party Relationships**. An inventory of third parties that collect data on behalf of Service Provider, handle or process Alnylam data or have access to Alnylam systems is documented and maintained, and accessible to Alnylam on Alnylam's request.
- **Lifecycle Management.** Service Provider must establish contracts with dependent suppliers providing material services; these contracts should incorporate security control requirements, including data protection controls and notification of security and privacy breaches. Review processes must be in place to ensure dependent suppliers' fulfillment of contract terms and conditions.
- **Third Party Monitoring.** Third parties are appropriately monitored for ongoing compliance with applicable laws and regulations, applicable policies and standards, and privacy and security obligations.

The aforementioned Minimum Control Requirements are expected to be complied with equally by all Service Providers, unless otherwise agreed in writing between Alnylam and such Service Provider.

Alnylam reserves the right to request that additional requirements are to be complied with for specific types of vendors, such as cloud service providers, or for specific type of processing activities, for example where the processing in question is likely to result in a high risk to the rights and freedoms of individuals, including but not limited to, for example, cases where sensitive data are being processed, or processing related to inherently vulnerable data subjects such as employees and patients.