UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

DOCUMENT CONTROL

This Section is to be updated, whenever this Document is updated after receipt at first instance by Company:

Author	External Legal (Vibha Oswal + Eqwiler Consulting)
File Name	IT Policy Company
Created	11th August, 2025
Last Edited	7 September, 2025

This policy will be reviewed annually or after any major operational/legislative change, and in the event of any incident regarding data retention policy.

UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

Information Technology

POLICY AND PROCEDURE MANUAL
AMAZON MARKETPLACE & MULTI-CHANNEL DATA HANDLING

This Policy governs the Information Technology processes, methods, scope, actions, to be implemented to ensure compliance with Applicable Laws (as defined hereinbelow in "Interpretations")

This policy applies to All employees, contractors, consultants, third-party vendors, and automated systems that access resources accessed by Unisouk including Amazon Marketplace resources, who are advised to read this Policy and check for updates from time to time. This policy shall form an integral part of all contracts entered into with contractors, consultants, third-party vendors, automated systems etc., and all obligations on such users shall be enforceable at law.

UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

INTERPRETATION

(1) **"*Amazon Data":*** Any data obtained through Seller Central, APIs, or reports from Amazon including customer data, order data, communications or any derivative information.

(2) "***Applicable Law***" shall mean and include all primary statutes, rules, laws, regulations, including the Digital Personal Data Protection Act and Amazon Data Protection Policy.

(3) "***Application Programming Interface***"or "***API***" : Rules and Protocols implemented by Company and / or Amazon Seller Account / Amazon Marketplace Account that permit Applications to share data and communicate with each other for the 'Business Purposes' of Company

(4) **"*API Materials*"** means Materials we make available in connection with the Amazon Services API, including APIs, documentation, specifications, software libraries, software development kits and other supporting materials, regardless of format.

(5) "***Data Security Officer***" or "***DSO***" Designated person responsible for Data Protection and Data Security governance identified and appointed by the Company.

(6) "***Developer***" refers to Unisouk in the process of rendering Services to its Customers.

(7) "***DPP***" means and refers to the Amazon Data Protection Policy, as updated from time to time on the official website of Amazon Marketplace.

(8) "***End User***" shall mean and refer to merchants who avail Unisouk's Services.

(9) "***Environment***" - In reference to PII, means and refers to the Amazon Marketplace Environment in which the PII originates, or is originally found in.

(10) "***Incident***" – An Incident is defined as any actual or suspected unauthorized access, acquisition, use, transmission, disclosure, corruption, or loss of Amazon Information or a breach of any system environment that handles Amazon Data.

(11) ***"Information Technology Resources***" or "***IT Resources***" include computing, networking, communications, application, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and related materials and services.

(12) ***"Information Technology Personnel" or "IT Personnel"*** refer to employees who are employed in the IT Department of Unisouk.

(13) **"*Materials*"** means software, data, text, audio, video, images or other Content.

(14) "***Multi Factor Authentication***" or "***MFA***" : an additional authentication method beyond a password**.**

(15) "***Other Channel PII***" or "***OPII***" shall mean and include any data, information which has been obtained by the Company from its other channels, including but not limited to channels such as ODC, independent marketing channels, marketing consultants, databases.

(16) "***Personally Identifiable Information***" or "***PII***" in context of 'Amazon Data' : means and includes any/ all data, information which can be utilized, whether in isolation or in combination with any other data to identify the customer, whether by their name, by their location, by their behaviour, by their preferences. which originate from Customers, Interface etc. of Amazon Market Place which includes customer names, IP Address, Customer Address, Chats/ Messages / Interactions with Customers, Customers' Activity on WebPage, Customer Behaviour etc. - and includes any textual reference to the term 'PII' in the Amazon Marketplace Policy.

(17) "***Role***" means the individual role allotted to the Employee as per the Job Description, and other matters mentioned in the employee contracts.

(18) "***Role Based Access Control***" or "***RBAC***" refers to authorization to end users in the system, and control of access to the system, based on individual role, and rules set in this Policy.

(19) "***Remote Access***" – Systems, Software and Hardware that permit authorized users to connect to and utilize Unisouk's internal network, systems and data from a location that is situated outside the physical office

(20) "***Service"*** shall refer to services of Unisouk including e-commerce SaaS platform offering unified multi-channel integration (Amazon, Flipkart, ONDC, websites), order and inventory management, AI-powered analytics, no-code store builder, and dashboard-based operations

(21) "***Third Party***" – Any independent third party or external entity other than Amazon, and Unisouk with whom Unisouk's IT Systems, data, or infrastructure interacts for the purposes of availing services by Unisouk.

(22) "***Third Party Tools***" refer to any tools, software, interface, or Third Party which interact with Unisouk's IT Systems, data or infrastructure.

(23) "***Internal User***" refers to any individual who has access to or utilizes Company's IT resources, including hardware, software, networks, data, and other technology-related assets.

ACCESS LIFECYCLE MANAGEMENT POLICY AND PROCEDURES

Data Security Officer to define clear access levels in the Organisation, and such access levels that each department is entitled to shall be clearly communicated to the employees.

UniSouk shall implement strict Access Management controls to ensure that access to Amazon Data is limited strictly to authorized personnel based on the principle of least privilege. All user accounts shall be provisioned in accordance with Role-Based Access Control (RBAC), granting only the minimum level of access required to perform assigned responsibilities. Shared, temporary, or generic accounts shall be expressly prohibited. Strong password policies shall be enforced, together with Multi-Factor Authentication (MFA) for all users

accessing systems handling Amazon Data. Access privileges shall be reviewed no less than once every calendar quarter, and the results of such reviews shall be documented and made available for Amazon audit. User accounts of terminated or inactive employees, or of those whose role changes no longer require access, shall be revoked immediately. Duties shall be segregated such that no single individual can request, approve, and deploy their own access rights, and developers or testers shall not be permitted to access live Amazon PII. All access attempts, both successful and unsuccessful, shall be logged, actively monitored, and reviewed for anomalies, with alerts configured for suspicious activity. Third-party access, including that of contractors or outsourced developers, shall not be permitted without prior approval, the execution of binding contractual safeguards, and implementation of strict technical controls ensuring access only to masked or limited environments.

Illustration:

Role	Access Scope
Admin	All functions including user management and policy changes.
Order Fulfillment	View and update order/shipment data; no customer email view.
Customer Service	Access to customer communications and limited order details.
Finance	Access to settlement reports and payment statements only.

ONBOARDING INTERNAL USER:

(1) Unisouk's HR / Hiring Manager corresponding to the role of proposed user, to submit E-mail request for IT access to proposed User to DSO for review. The E-mail request is to consider details of (i) job description / role of proposed User (ii) access level requested for proposed User. This can be managed by e-mails or through an access request form developed for this purpose.

(2) In the event the requested access includes access to Environment where Amazon Data and PII are found, then DSO to request HR to provide details of background check and screening.

Note: As per Amazon DPP, identity of employee, employment history and red flags are to be identified.

(3) Upon HR confirmation of identification, employment history, address verification etc., DSO to business need to grant level of requested access and grant permission to IT to provide the requested access.

(4) Access to Amazon Marketplace data shall be restricted to designated teams only, based on business need and in compliance with the Amazon DPP:

(a) **Engineering Team** – limited to functions involving system integration, development, and maintenance of platform infrastructure.

(b) **Legal & Compliance Team** – limited to functions involving regulatory compliance, contract review, dispute resolution, and Amazon policy enforcement
(c) **Technical Support Team** – limited to functions involving troubleshooting, order support, and customer issue resolution.

Within each team, the DSO) shall apply the principle of least privilege and assign role-based access strictly necessary for the performance of duties. All access shall be logged, reviewed quarterly, and revoked immediately upon role or team change.

(5) Implementation of Least Access – Least Privilege Protocols: i.e. granting minimum level of access and privileges. Privileges will be limited to the minimum necessary for an individual to perform their role. (DSO to adhere to Rider of *Least Access – Least Privilege* while deciding access level granted to any User)

(6) Internal Users are granted strictly the minimum level of access and privileges necessary to perform their duties.

(7) User Accounts shall be automatically suspended in event of inactivity for a period of 90 (Ninety) days.

(8) Internal Users must complete Amazon DPP training before first login.

(9) Internal Users shall only use company-owned devices.

(10) Every Internal User must have a unique login, shared accounts shall be prohibited.

(11) MFA shall be mandatory for (a) all administrative accounts, (b) Amazon Seller Central Access (c) Remote Access to internal systems (d) Access to Customer Data Systems

(12) IT to enforce Attribute-Based Access Control (ABAC) or Role-Based Access control (RBAC) to enforce access limits.

(13) IT to implement Security Information and Event Management System.

(14) Audit Logging: For Purposes of complying with Amazon's Audit, IT System should have all features enabled for an activity log showing accurately, the activity, access, and duration of access of Amazon Data.

Note: For Effective Activity Monitoring: Create roles like: amazon_ops_user, Internal_data_analyst with tags that reflect the job roles, responsibility and can be used by DSO to identify business need of access.

(15) IT to make access to sensitive information based on elevated privilege which shall be granted on a strict time line basis. IT to Monitor Access Logs for all privileged activities.

(16) DSO to ensure not to give one person full control. No Single Internal User to be assigned multiple roles.

(17) Segregation of Duties: Each Internal User shall be assigned roles and responsibilities in a manner that ensures segregation of duties, prevents conflicts of interest, and minimizes security risks. A User shall not simultaneously hold multiple roles where such combination could compromise security, data integrity, or compliance with the Amazon Data Protection Policy ("Amazon DPP").

(18) Prohibition on Conflicting Roles: Users shall not be assigned conflicting roles (including but not limited to roles involving system administration, security monitoring, and data processing functions) unless an exception is expressly approved in accordance with Section 3 below.

(19) Exceptions Process: Any exception to the prohibition on conflicting role assignments must be:

(a) documented with clear business justification;
(b) approved in writing by the Data Protection Officer (or other designated compliance authority); and
(c) accompanied by compensating controls (e.g., heightened monitoring, logging, or independent review) to mitigate associated risks.

(20) A record of all exceptions, including justification, approvals, and compensating controls, shall be maintained and made available to Amazon upon request.

(21) Review and Monitoring: Multi-role assignments shall be reviewed at least quarterly by the Data Protection Officer (or designated authority) to confirm ongoing necessity and adequacy of risk mitigation measures. Any expired or unjustified multi-role assignment must be revoked immediately.

(22) Unisouk shall review all accounts and privileges on a six monthly basis and maintain reports of all reviews, with identified issues and actions taken thereof.

CHANGE IN ROLE:

(1) In case of change in role of Internal User, Access protocols must be updated immediately to reflect the change in role of Internal User. At all times, access to any Environment/ Repository must be justified by clear business need which is associated and linked to the Internal User's Job Role.

(2) User cannot be onboarded on any new Role unless Access is expressly permitted by DSO to that particular Internal User. DSO to strictly adhere to Least Access Rider while changing any Access / Role of Internal User.

UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

OFFBOARDING INTERNAL USER:

(1) HR shall submit a request to IT requesting revocation of access to Internal User, in the request submitted by HR, HR shall confirm the termination date or last date of contract with the employee.

(2) Within 24 hours of receiving a request for revocation of access, access of such Internal User is to be revoked.

(3) IT shall ensure that (i) All credentials disabled, (ii) tokens revoked, and devices (iii) All Activity and Access Log is preserved for inspection and (iv) returned or wiped. IT shall check Activity and Access Log and flag any event of mass downloads, or access outside of working hours, and inform the DSO.

(4) DSO shall review the flagged activity as per the clause above, and in event of any concerns of data leaks, breach of confidentiality etc. DSO shall alert the Legal Officer within 24 Hours of such identification of data leak, breach of confidentiality etc.

(5) No Relieving / Experience Letter to be given unless and until the Access Revocation actions as stated herein are completed.

REMOTE ACCESS POLICY:

(1) IT shall provide limited access strictly necessary for performing the Role assigned to the Employee.

(2) Internal Users shall not use Wi-Fi without using authorized VPN.

(3) Access Management shall be governed as per this Policy at all material times.

(4) Access to Amazon Marketplace data will be granted strictly on a need-to-know basis, justified by a clear business need.

(5) No Single Internal User shall be assigned multiple roles without written consent of the DSO.

(6) Internal User Access should be monitored regularly

(7) IT to enforce appropriate access controls that prevent mass downloads of data

(8) IT to enforce appropriate access controls and protocols to prevent access to PII

(9) Roles are defined with clear permissions.

Examples:

(a) Admin: Full account management, policy updates, order management, data reporting.
(b) Order Fulfillment: Order and shipping data access only.
(c) Customer Service: Limited access to order and communication data.
(d) Finance: Access to payment reports and settlement data only.

(10) One of the objectives of the IT Systems, over a five year period, is to ensure added protection of IP-Based Access Control in addition to Role Based Access Control.

PII HANDLING PROTOCOL

(1) At all material times, the Company shall isolate, separate, in terms of storage and resources that access the storage, Data received via Amazon vis-a-vis Data received from other channels such as website, ONDC, marketing efforts etc.

(2) The Company shall adopt strict separation in handling PII from various channels. The Company is authorized to access data on behalf of its Customers, which originate from various sources, including Amazon, ONDC, website and other such channels.

(3) The Source of collection shall dictate how data is to be used. There shall be no cross use of Amazon Data whether for marketing, CRM enrichment, analytics outside of Permitted Use, or cross channel profiling. Amazon Data can only be used for order fulfilment, customer service and legal compliance related to the corresponding Amazon transaction. Permitted Uses shall include order fulfilment, returns, refunds, legal compliance and customer service obligations. Prohibited Uses include any use apart from Permitted Use.

(4) Amazon Data must be stored and processed in logically or physically separated systems. The Company may process Website Data, ONDC Data etc. together, subject to general data protection laws and the privacy policy of the Customer.

(5) The Company shall only collect and process PII from Amazon Data necessary for the purpose of Order Fulfilment and legal compliance corresponding to that particular transaction.

(6) Access to Amazon Data shall be granted only to Internal Users/ systems involved in order fulfilment or support.

(7) Unisouk shall implement Multi-Factor Authentication (MFA) for all logins to Seller Central and associated systems.

(8) The Company shall at all times comply with Amazon Data Retention Period as mandated by Amazon DPP. The Company shall delete Amazon Data within Thirty Days post Order fulfilment unless required by law. All Data tagged as 'Amazon' is to be set to auto-delete within 30 Days after Date of Order Fulfillment / Purpose Fulfillment .

(9) Unisouk does not maintain any backup of Amazon Data.

(10) The Company does not have any conflicting policies to the Amazon DPP in respect of Amazon Data. However, the Company may use Website Data, ONDC Data subject to data protection laws, and privacy policy. The Company treats each data set according to its collection source, and all Amazon-sourced data i.e. Amazon Data is used strictly for Permitted Uses, in alignment with Amazon DPP.

(11) Data originating from Amazon systems, APIs, reports, or order notifications to be tagged is required to be tagged as 'Amazon Data' and maintained in encryption at rest.

(12) The Company generally encrypts all Amazon Data, PII in transit and at rest.

(13) The Company shall maintain Logs of Internal Users who have accessed Amazon Data, for purposes of Audit Preparedness.

DATA GOVERNANCE AND DATA MAPPING

(1) Purpose: Unisouk maintains a data governance framework to ensure that all Amazon Data is collected, processed, stored, and deleted in compliance with the Amazon DPP and applicable data protection laws. This framework documents the flow of Amazon Data within Unisouk's systems and ensures transparency, accountability, and audit readiness.

(2) Data Collection and Use:

(a) When Sellers connect their Amazon accounts to the Unisouk Platform, access is granted exclusively through Amazon's secure login and authentication mechanisms (OAuth or API).

(b) Unisouk collects only the minimum fields of Amazon Data necessary for the following permitted purposes:

(i) Order fulfillment and shipping.
(ii) Customer support and dispute resolution.
(iii) Returns, refunds, and replacements.
(iv) Compliance with statutory, tax, and accounting obligations.

(c) In accordance with the principle of data minimization, no additional fields shall be collected beyond what is strictly required for the permitted purposes. Data accuracy shall be validated against Amazon's API protocols to ensure integrity.

(d) Amazon Data shall not be used for analytics, profiling, marketing, or any other purpose outside the Permitted Purposes.

(3) Data Flow and Segregation

(a) Amazon Data flows directly from Amazon Seller Central into Unisouk's secure environment via approved APIs.

(b) All Amazon Data is encrypted in transit (TLS 1.2+) and at rest (AES-128 minimum, with migration to AES-256 in future).

(c) Amazon Data is logically and technically segregated from all other categories of data, including ONDC Data, Website Data, and Marketing Data. At no stage shall Amazon Data be combined, cross-referenced, or commingled with such other datasets.

(d) Access to Amazon Data is limited to authorized teams only and always on a least-privilege basis. Access rights are reviewed quarterly by the DSO, and all access is logged for audit purposes.

(4) Retention and Deletion

(a) Amazon Data shall be retained only for as long as necessary to complete the relevant fulfilment process plus thirty (30) days, unless a longer retention period is required by applicable law.

(b) Upon expiry of the retention period, Amazon Data shall be securely deleted through cryptographic erasure or equivalent secure methods.

(c) Deletion logs shall be maintained by the IT Team and reviewed quarterly by the DSO to verify compliance with this Policy.

(5) Documentation and Audit

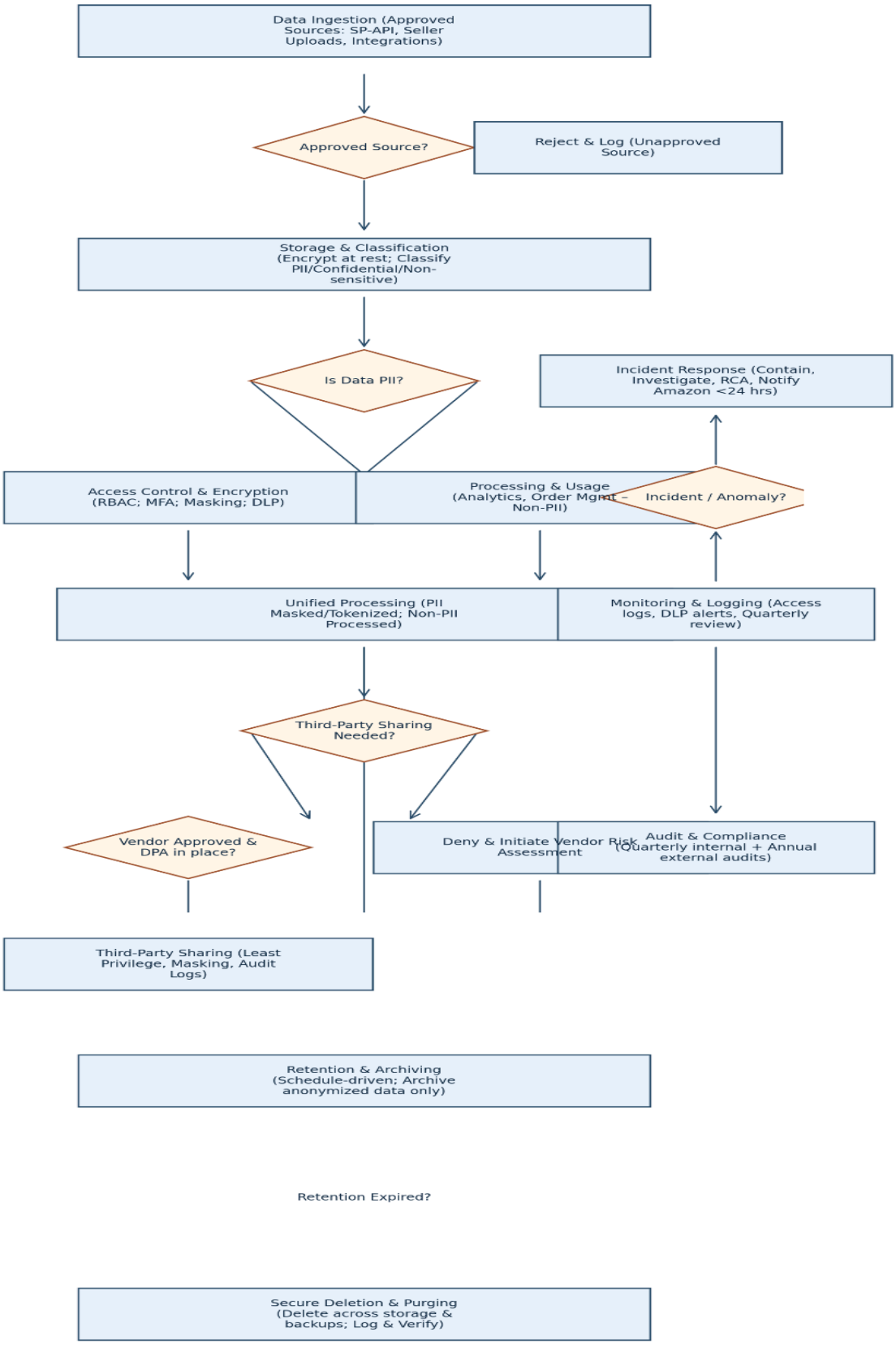
(a) Unisouk shall maintain internal documentation of:
(i) All fields and API endpoints accessed.
(ii) Process and data flow diagrams illustrating the lifecycle of Amazon Data.

(b) This documentation shall be treated as internal compliance annexes, updated at least bi-annually or immediately upon any change in Amazon APIs, system integrations, or legal requirements.

(c) Such documentation shall be made available to Amazon or regulators upon request, as evidence of compliance with the Amazon DPP.

UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

UniSouk Data Governance Workflow (Amazon DPP-aligned)



UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

Workflow Steps for Amazon Data

(1) Data Ingestion (Approved Sources: SP-API, Seller Uploads, Integrations)
(2) Approved Source? If No → Reject & Log; If Yes → Continue.
(3) Storage & Classification (Encrypt at rest; Classify as PII/Confidential/Non-sensitive).
(4) Is Data PII? If Yes → Apply Access Control & Encryption (RBAC; MFA; Masking; DLP). If No → Process directly.
(5) Unified Processing (PII Masked/Tokenized; Non-PII processed).
(6) Third-Party Sharing Needed?
    a. If Yes → Vendor Approval & DPA required. - If Vendor Approved → Third-Party Sharing with masking, least privilege, audit logs. -
    b. If Not Approved → Deny & Initiate Vendor Risk Assessment.
(7) Retention & Archiving (Schedule-driven; Archive anonymized data only).
(8) Retention Expired? If Yes → Secure Deletion & Purging across systems and backups (logged and verified).
(9) Monitoring & Logging (Access logs, DLP alerts, Quarterly review).
(10) Incident/Anomaly Detected? If Yes → Incident Response (Contain, Investigate, RCA, Notify Amazon <24 hrs).
(11) Audit & Compliance (Quarterly internal + Annual external audits).
(12) End / Completion of lifecycle.

Workflow Steps for Generalized Handling Data as per Data Protection Laws

(1) Step 1. Collect Data with Consent
    (a) Valid consent or lawful ground
    (b) Privacy notice provided
    (c) Only necessary data collected

(2) Step 2. Store & Classify Data
    (a) Encrypt at rest
    (b) Classify: PII / SPDI / Non-Personal
    (c) Store in approved environment

(3) Step 3. Control Access
    (a) Role-based (RBAC)
    (b) MFA + logging
    (c) Quarterly access reviews

(4) Step 4. Process Data Lawfully
    (a) Use only for consented purpose
    (b) Mask/anonymize where possible

(c) No unauthorized profiling

(5) Step 5. Share / Transfer Data Securely
- (a) DPA with vendors
- (b) Cross-border rules followed
- (c) Only approved vendors

(6) Step 6. Retain Data Only as Needed
- (a) Minimum retention
- (b) Archival in anonymized form
- (c) Automatic deletion.

IMPLEMENTATION OF MEASURES IN COMPLIANCE WITH AMAZON DPP

(1) Unisouk prohibits use of Amazon Data, PII and other personally sensitive information in testing, production and QA Environments. Unisouk observes a strict policy of permanent data anonymisation which renders data such that it cannot be used to identify any individual.

(2) PII in Amazon Data shall be displayed only to the extent necessary and Unisouk adopts Data Masking Policy based on least privilege within the pool of Internal Users who are permitted to access Amazon Data for the purposes of order fulfilment.

(3) Unisouk automatically anonymizes PII in log files. Unisouk expressly prohibits de-anonymization by any Internal User, and in the event any attempt to De-Anonymize is identified during Audits, DSO shall take strict disciplinary action, including termination against the individual identified as responsible.

(4) It shall be ensured that Amazon Data and PII are encrypted at rest and in transit.

(5) Permitted Uses of Amazon Data:
- (a) Order Look Up
- (b) Logging E-mail Addresses during Order Processing
- (c) Refunds/ Returns
- (d) Cancellations
- (e) Customer Service
- (f) And such other uses as may be allowed under the Amazon DPP or applicable laws.

(6) All Internal Users are expressly directed to exercise highest standard of care and precaution and Unisouk explicitly prohibits:
- (a) Clipboard Copy-Paste of Amazon Data into non approved applications is strictly prohibited.
- (b) Accessing Back-End Data Bases
- (c) Exporting Customer Data to Excel or CSV
- (d) Temporary Access to Employees who are not cleared to access Amazon Data, PII

(e) Screenshots, Screen Recordings and other modes of Screen Capture
(f) Using PII Fields in Unit Test Scripts
(g) Use of Customer Addresses in API responses
(h) Static Customer Data / PII scrubbing
(i) Logging user IPs with names and order info outside the Environment
(j) Joining PII fields to any external database
(k) Hardcoding PII values for feature testing
(l) Displaying full buyer information in admin panels
(m) Using production data in QA environments
(n) Testing customer notification features with live emails
(o) Refrain from Sharing Real Order Data between QA teams and instead use Reference and Identification Numbers generated on the Environment
(p) Mask PII in Automated Screenshots
(q) Writing Automated UI tests that reveal buyer names
(r) Export test results with Embedded Customer Details
(s) Running Performance Tests that Exposure Sensitive Fields
(t) Replicating Customer Issues using real PII
(u) Failing to Anonymize Test Case
(v) Accessing test Data Bases with Live Customer Data
(w) Sending customer data to third-party analytics tools
(x) Technical safeguards to prevent passing of Order Information to ERP systems
(y) Integrating with Customer Support Tools without Masking
(z) Technical Safeguards to ensure Outsourced Developers do not access live PII
(aa) Technical Safeguards Preventing Business Integrated Tools from caching sensitive Information

(7) Any information of suspected breach must be reported to DSO within 1 hour of suspicion arising. DSO to immediately investigate and evaluate criticality, existence of risk, potential damage and to issue a report of findings and take all remedial action within 7 (Seven) Days of the breach being identified.

(8) Unisouk strictly restricts access to PII must be by Role Based Access Control in addition to mandatory Identity Verification Based Access to all Hardware Devices and Software Resources.

(9) PII on the Amazon Marketplace should not be exported out of the environment in which the data is originally found. Implementation of controls to prevent exporting data in Excel or CSV, or in any other format is mandatory.

(10) UniSouk shall not maintain any backup of Amazon PII outside the approved Environment. All backups of Amazon PII within the Environment shall be encrypted at rest using industry-standard encryption (AES-128 or equivalent), access-controlled, and subject to the same security requirements as production data. Backups shall be retained only for the minimum period necessary for business continuity and shall be deleted upon expiration of the retention period or upon request by Amazon. Deletion shall extend to all backup copies to ensure complete removal of PII. All backup activities shall be logged and available for Amazon audit.

(11) Even under exceptional circumstances, temporary database access/ database access shall not be provided to non-cleared employees, as set forth in this Policy.

(12) The Company ensures that the Marketing Data received from other channels such as Website, ONDC, etc. shall be obtained by express consent only. The Company should not indulge in data scraping, or any other methods of data collection which may raise apprehension or doubt of being obtained without express consent.

(13) In case of any conflict, the Company, Amazon DPP shall accord higher priority, and the Company must abide by Amazon DPP only.

(14) The Company does not use any internal or external scripts, and no part of the Scripts used by the Company processes PII.

(15) The Company will not build separate Applications to access the Shipping Labels except for the limited purposes of Order Fulfilment

(16) Internal Users to avoid Returning full customer names in UI debug mode

(17) Internal Users cannot share reports with external consultants

(18) Internal Users shall not take screenshots and shall not share screen shots of labels for internal issue reporting.

(19) Internal Users shall not include PII in Order Summary Exports

(20) Internal Users shall not have open access to label printing tools

(21) Internal Users shall share limited order details to warehouses for order processing.

(22) DSO shall take all necessary precautions against misclassifying PII as non-sensitive.

(23) IT shall enforce all necessary system controls, specifications, etc. which prevents (i) accessing label databases without audit trail (ii) sharing tracking sheets with all buyer fields (iii) attaching shipping manifests with customer contact information

(24) IT shall look for PII breaches in bug bounty.

SOFTWARE DEVELOPMENT LIFECYCLE POLICY

(1) Purpose and Scope: This Section of the policy lays down the guidelines for development of software, testing, debugging, code changes, configuration updates, production deployment etc.

(2) Plan and Approval: Unisouk creates clear requirements in a planned manner, in accordance with security, data privacy, and compliance perspective, prior to designing any software for Unisouk.

(3) Unisouk shall always adhere to Security by design embedding best standards and practices in all phases of development.

(4) Unisouk embeds encryption, data segregation, PII controls and secure integrations in its processes.

(5) Unisouk maintains a clear list of Vendor Dependencies, and controls access to each such API separately.

(6) The Coding and Developing team shall follow secure coding practices, and use protections and mandatory code review.

(7) Only members of the Coding and Developing Team shall have access to the environments where the code is being hosted or developed, especially for data sensitive components.

(8) Regular and Ad-Hoc Functional Testing to be carried out, including security scans, vulnerability scans, code reviews and penetration tests as per terms set out herein.

(9) Unisouk carries out six monthly vulnerability scans on all production systems. Further, Unisouk shall also carry out additional scans after any major infrastructure or application change.

(10) Unisouk utilizes automated scanning tools which are recognized, accredited and aligned with industry standards and benchmarks such as OWASP, NIST etc.

(11) Unisouk maintains a log report of all scan reports in a Security Register, and findings of the security scans are to be categorized by severity in the scan reports which are issued after each scan tests.

Critical	Vulnerabilities allowing remote, unauthenticated exploitation or compromise of Amazon Data, system availability or encryption mechanisms. Common Vulnerability Scoring System CVSS 9.0-10.0
High-Risk	Vulnerabilities that require some level of authentication or user interaction but still allow significant compromise of data or systems. Common Vulnerability Scoring System CVSS 7.0-8.9
Medium Risk	Vulnerabilities that partially impact security but require specific conditions, multiple exploit steps, or insider access to be successful. Common Vulnerability Scoring System CVSS 4.0-6.9
Low Risk	Vulnerabilities that have minimal security impact or relate primarily to best practices, without direct data compromise potential. Common Vulnerability Scoring System CVSS 0.1-3.9

(12) Unisouk shall remedy all Critical Vulnerabilities within 7 Days, High Risk Vulnerabilities within 10 Days, Medium Vulnerabilities within 15 Days and Low Risk Vulnerabilities within 30 Days.

(13) Unisouk shall undertake re-testing before marking Vulnerabilities as resolved.

(14) The Team shall dedicatedly track progress on remediation of each vulnerability until closure of all identified issues.

(15) Unisouk shall appoint an external third party independent certified provider to conduct annual external penetration testing. Unisouk shall also appoint such independent certified providers to conduct additional testing after major code releases, infrastructure upgrades or incidents.

(16) Results from scans, penetration tests etc. shall be used to update secure coding guidelines, enhance SDLC practices, strengthen monitoring and defensive controls.

(17) IT Security Head to approve Penetration Test Reports, documented corrective action plans, and closure of vulnerabilities by re-testing before marking the Vulnerabilities as resolved.

(18) The Team shall implement and adhere to strict PII Handling protocol, and all PII and Seller Data shall be encrypted at rest and transit using TLS 1.2+ and AES-128 with a plan to upgrade to AES-256 in the next six months.

INCIDENT RESPONSE POLICY AND INCIDENT RESPONSE PLAN

(1) This Section of the Policy shall be reviewed on a bi-annual basis by an external IT & Legal Consultant, and shall be reviewed and updated contemporaneously to every update to Amazon DPP hosted on the Official Amazon Website. TL; DR: Review Incident Response Policy on an annual basis and immediately after any update to DPP.

(2) Unisouk shall appoint an Incident Response Team under the DSO or a future incident response commander. The Incident Response Team shall perform the following function: (i) Access all systems and data necessary for incident investigation (ii) Temporarily restrict system access or functionality during incident response (iii) Coordinate with external parties including law enforcement and vendors and (iv)Direct all incident-related communications, (v) Isolate affected systems within 1 hour of confirmation Implement immediate containment measures to prevent spread (vi) Preserve forensic evidence before system restoration and (vii) Maintain detailed logs of all containment activities

(3) IT Personnel who are the first to identify, or recognize any Event within 2 Hours of Discovery to the DSO.

(4) DSO will evaluate the Event and immediately take all investigations to identify whether any PII or Amazon Data is involved in the Event, and enforce appropriate Incident Response as stated in the Incident Response Policy hereinabove.

(5) Within 24 hours of detection or suspicion of an incident, notify Amazon at Use 3p-security@amazon.com or security@amazon.com to intimate Amazon of the Incident.

Note: DSO to be prompt in responding to Information Requisitions, as delays carry risk of API Access.

(6) DSO to undertake Risk Identification, based on following matrix:

CRITICAL	System outage, confirmed data breach, ransomware	CEO, Legal, DSO
HIGH	Unauthorized access, malware detection, service disruption	DSO, Legal
MEDIUM	Suspicious activity, policy violations with security impact	DSO
LOW	Failed intrusion attempts, minor policy violations	DSO

(7) Incident Response Team shall notify Executive leadership within 2 hours in case of Critical/High incidents

(8) Incident Response Team shall direct IT Team to preserve system state and shall not shut down any systems for accurate incident reporting and investigation. Incident Response Team shall direct IT Team to preserve all evidence pertaining to the incident.

(9) DSO shall assign team to Investigate thoroughly and (i) Description of the Incident to be submitted in writing to DSO, (ii) DSO and Admin to submit Remedial Actions to be taken within 3 days i.e. 72 Hours of the Incident,

(10) Corrective controls to be implemented to prevent recurrence, Follow approved system restoration procedures

(11) Verify security controls before returning systems to production

(12) Include monitoring for recurring incidents

(13) Document lessons learned within 5 business days

(14) Regular status updates every 4 hours during active incident response

(15) In the event of any suspicion that Amazon Data or Amazon PII is breached

(a) DSO to address correspondence to Amazon notifying Amazon of the suspected breach
(b) Access Logs are 30 days are good to have
(c) At all times, Company should be able to track all personnel who had admin access to Data
(d) Provide a Detailed Report on Data Accessed during Incident, and details of response and remedial actions taken by Company

(16) Do an Incident Response Drill to ensure Preparedness, identify gaps during Drills, and take corrective actions

(17) In the event that business website is disrupted, the following actions must be immediately undertaken:

(a) Notification to Website Host
(b) Identification of any Data loss caused by disruption,
(c) Temporarily Unpublished Website for duration of Trouble-Shooting
(d) Chain of Custody to be Maintained & Evidence Preservation:
  (i) Maintain Evidence and Audit Logs in a manner that preserves integrity and enables verification.
  (ii) Logs Proof are Tamper - Proof and securely stored.

(e) Do not notify any third party (e.g. customers, regulators) without Amazon's explicit prior written consent.
(f) Co-operate fully by providing all relevant data / information as requested - such as Access Logs, API Logs, Audit Trails, Error Logs, Server Configurations, Software Versions, Patch Levels, Internal Incident Analysis, Timeline, Remediation Actions Taken, Names and Roles of Individuals who had access to Amazon Data, Subcontractor and Service Provider details, Screenshots, Memory Dumps, Log Extracts, E-mail Trails etc.
(g) Investigate scope of exposure, impact on Amazon Customers/ Sellers, Trigger of Legal / Contractual
(h) Conduct thorough investigation for Privacy Compliance
(i) Change Passwords of Amazon Marketplace
(j) Incident Records are to be maintained for a period of Seven Years, and in case of any legal hold request from Amazon to treat the data as Forensic Evidence, the Incident Records are to be retained for a period of Seven years.
(k) In the event any User is identified to have been responsible for, or caused any such Incident to take place, Unisouk shall initiate disciplinary action up to and including termination, civil and/or criminal liability for wilful violations and claim for damages.

Note to Unisouk:

'People are the first line of defense – or the weakest link'

Incidents to Data may be due to external factors and internal factors, internal factors usually involve human element, and to ensure that risk from internal factors is minimized to zero strictly follow Access Management Policy, Remote Access Policy, Background Checks during Hiring and ensure regular Security Awareness Training.

UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

PASSWORD AND API KEY POLICY

(1) Purpose: This policy establishes the requirements for secure creation, storage, rotation, and monitoring of passwords and API keys in compliance with the Amazon Data Protection Policy (DPP) and industry best practices.

(2) Unique Password for Amazon Seller: Amazon Seller Account Password shall not be used anywhere else.

(3) Amazon Seller Password must be updated every 60 (Sixty) Days, except for Immediate Change in Password as Per Incident Response Plan. API Key to be rotated every 90 (Ninety) Days.

(4) Password Authentication to be accompanied by MFA at all times for all Seller Central and API.

(5) Passwords must be 12+ characters, a mix of upper/lowercase, numbers, special characters.

(6) Use Complex Passwords:

(a) Random String of Mixed Case Letters, Numbers, and Symbols, or
(b) Use Unrelated Phrases.

(7) Passwords shall not be Re-Used.

(8) Accounts shall not be shared.

(9) Internal Users shall be permitted to use Password Managers, provided such Password Managers are obtained by Licensed Sellers. Users shall not store the passwords on word documents.

(10) In the event any Internal User changes password, they shall not be permitted to change their password again for a period of 24 (Twenty-Four) Hours from the previous change.

(11) All Internal Users are instructed to exercise care and precaution of privacy while entering their credentials. Storage of any credentials in plaintext format is strictly prohibited.

(12) In the event any Internal User enters or provides incorrect or invalid credentials for a period of five continuous instances, their account shall be immediately locked after the fifth consecutive instance, and the IT Administrator shall re-instate access only upon written request of the Internal User.

(13) Every Internal User must have an individual account with unique credentials.

(14) API Key Policy:
(a) Keys must be system-generated, never user-created or hardcoded.
(b) Keys must not be exposed in code repositories, scripts, or config files.
(c) Distribution only through encrypted vaults/secret managers.

(15) Storage & Protection
- (a) Keys stored only in AWS Secrets Manager, HashiCorp Vault, or equivalent.
- (b) Encryption at rest: AES-128 or stronger.
- (c) Encryption in transit: TLS 1.2+.

(16) Rotation & Revocation
- (a) Keys rotated at least every 90 days.
- (b) Keys revoked and replaced immediately upon compromise or when access is no longer required.

(17) Access & Usage
- (a) Keys must be uniquely assigned (no shared credentials).
- (b) Scoped permissions applied (least privilege).
- (c) Unused or expired keys must be deactivated promptly.

(18) Audit & Monitoring
- (a) All key usage must be logged (success, failure, attempted access).
- (b) Logs must be retained for 12 months in line with Amazon DPP.
- (c) Automated alerts for suspicious or unauthorized activity.

(19) Enforcement & Responsibilities

Security Team / CISO: Maintain and enforce this policy, perform regular audits, and ensure compliance with Amazon DPP.

- (a) System Administrators: Implement technical controls for password hashing, secret storage, encryption, and monitoring.
- (b) Developers: Ensure API keys are never hardcoded or exposed in code repositories.
- (c) Employees & Contractors: Follow this policy when handling credentials.

(20) All employees with access to Amazon Information must undergo annual security training covering password and API key handling.

(21) Monitoring & Auditing

- (a) Credential use will be monitored continuously.
- (b) Quarterly internal audits will be performed to ensure compliance.
- (c) Evidence of compliance will be retained for Amazon audit requests.

DATA REQUEST POLICY

For the purposes of this Section, the following terms shall have the following meanings:

(1) Receipt of Request

(a) Any request from a Data Subject concerning access, rectification, or erasure of Personal Data shall be deemed valid upon receipt through designated channels (email, web form, or physical submission).
(b) The Data Fiduciary shall acknowledge receipt within seven (7) business days of such request.

(2) The request shall be logged in a Data Subject Request Register, recording:
(a) Identity of the Data Subject,
(b) Nature of the request,
(c) Date and mode of receipt,
(d) Assigned reference number.

(3) Verification of Identity
(a) The Data Fiduciary shall verify the identity of the Data Subject to prevent unauthorized disclosure.
(b) Verification may require government-issued identification, secure authentication, or equivalent means.
(c) If the request is made through an authorized representative, proof of authorization must be validated.

(4) Assessment of Request
(a) Upon verification, the request shall be reviewed by the Data Protection Officer (DPO) or an appointed compliance officer.
(b) The review shall assess: (i) Legitimacy of the request, (ii) Applicability of legal exemptions (e.g., public interest, legal obligation, ongoing investigation), (iii) Feasibility of the request without disproportionate impact on other data subjects or the business.

(c) 4.1. The Data Fiduciary shall provide the Data Subject with: (i) Confirmation whether their data is being processed, (ii) Categories of data, purposes of processing, recipients, retention period, and (iii) source of data.

(d) A copy of the personal data in a structured, commonly used, and machine-readable format.

(e) Fulfillment shall occur within thirty (30) calendar days from acknowledgment, subject to permissible extensions.

(5) Rectification Requests (DPDP Sec. 12)
(a) Where data is inaccurate or incomplete, the Data Fiduciary shall correct, update, or supplement such data without undue delay.
(b) If correction is not possible, reasons shall be provided in writing within the statutory timeline.

(6) Erasure Requests (DPDP Sec. 12)
(a) Where lawful grounds exist, the Data Fiduciary shall erase personal data, including backup and mirrored systems, unless retention is mandated under applicable law.

(b) Third parties with whom such data has been shared shall be duly notified of erasure, unless impossible or requiring disproportionate effort.

(7) Record-Keeping and Audit Trail

(a) All Data Subject Requests shall be documented, including: (i) Request details, verification steps, assessment outcome, and execution measures (ii) Any correspondence exchanged with the Data Subject.
(b) Records shall be preserved for a minimum of three (3) years for audit and regulatory review.
(c) An audit trail shall be maintained, capturing: (i) Timestamp of actions, (ii) Personnel responsible, (iii) Systems accessed or modified, (iv) Legal justifications relied upon.

(8) Communication of Outcome
(a) The Data Fiduciary shall communicate the outcome of the request in clear and precise language within statutory timelines.
(b) Where requests are denied, the Data Fiduciary shall provide a written explanation citing specific provisions of applicable law.
(c) The Data Subject shall also be informed of the right to escalate the matter to: (i) The Data Protection Board of India (DPB) under the DPDP Act, 2023, and/or (ii) The Supervisory Authority under GDPR.

(9) 7. Escalation & Appeals
(a) Data Subjects dissatisfied with the handling of their request may escalate the matter internally to the DPO within fifteen (15) business days.
(b) If unresolved, the Data Subject may approach the competent regulatory authority.

DATA RETENTION POLICY

(1) Unisouk does not collect and process data except to the extent for rendering Services to End Users. Unisouk adheres to strict data minimization and purpose limitation norms.

(2) Unisouk may collect certain data of its End Users, or Website Users for the purpose of providing its Services. In the event such End User or Website User is desirous of correction, completion, updation or erasure of their personal data, they shall reach out to the Grievance Officer whose credentials are provided below with particulars of their request, which shall be processed within a period of 30 (Thirty) days. In the event Unisouk is not able to process the request within 30 (Thirty) Days, Unisouk shall intimate the End User or Website User of the extension so required, and if the data is required to be retained for Income Tax Law, financial book-keeping obligations and other such regulatory compliances, Unisouk shall have the right to refuse complying with such a request.

(3) Data Category and Sensitivity Level to be identified by Classification Levels (i) ***Critical*****:** Amazon Data, Legal, Financial, Tax Records, (ii) ***Important***: Customer Data, Business Operations, (iii) Standard: Internal communications, analytics, (iv) ***Temporary:*** logs, cache files, temporary processing data. Retain only Temporary: Logs, cache files, temporary processing data (short retention)

(4) Once Data Category and Sensitivity Level is identified, such data must be tagged based on sensitivity level.

(5) Unisouk already implements a strict thirty day retention and thereafter permanent deletion with respect to Amazon Data which is handled as per the PII Handling clauses in this Policy.

(6) Unisouk to collect and retain only data that is adequate, relevant and limited to what is necessary for the business purpose. Unisouk implements the following data retention mechanism which are critical and are required to be adhered, observed and followed at all material times.

Data Category	Retention Period	Legal Basis	Disposal Method
PII in Amazon Data	Order Fulfilment + 30 Days	Order Fulfilment	Secure Deletion + Auto Deletion
Customer Order Records	7 years	Tax compliance, warranty claims	Secure deletion
Shipping Information	3 years	Business operations, returns	Secure deletion
Customer Communications	3 years or case closure	Customer service, disputes	Secure deletion
Payment Transaction Logs	7 years	Financial regulations	Secure deletion
Return/Refund Records	7 years	Tax compliance, accounting	Secure deletion
Product Review Data	5 years	Business intelligence	Anonymization
Amazon Seller Account Data: (i) Performance metrics	2 years	Business intelligence	Secure deletion
Amazon Seller Account communications	7 years	tax compliance	
Amazon Seller Account Marketing Campaign Data	3 Years	Marketing	

IT System Data

Data Category	Retention Period	Legal Basis	Disposal Method
System Access Logs	1 year	Security monitoring	Automated deletion
API Logs	90 days	Security monitoring	Automated deletion
Integration Test Data	No Retention	Testing	Automated deletion
System Configuration Backup	1 Year		
Security Incident Records	7 years	Legal compliance	Secure archival
Backup Data	3 months	Business continuity	Secure deletion
Email Communications	3 years	Business operations	Secure deletion
Network Traffic Logs	90 days	Security analysis	Automated deletion

Marketing Data

Data Category	Retention Period	Legal Basis	Disposal Method
Email Marketing Lists	2 years after opt-out	Consent management	Secure deletion
Website Analytics	14 months	Business optimization	Automated deletion
Customer Behavior Data	2 years	Legitimate business interest	Anonymization
A/B Testing Results	3 years	Product development	Anonymization
Social Media Analytics	1 year	Marketing analysis	Secure deletion

Internal Business Data:

Data Category	Retention Period	Legal Basis	Disposal Method
Employee Records	7 years post-employment	Employment law	Secure deletion
Contractor Agreements	10 years post-completion	Contract law	Secure deletion
Financial Statements	10 years	Accounting regulations	Secure archival
Tax Documentation	7 years	Tax law requirements	Secure archival
Audit Records	7 years	Regulatory compliance	Secure archival
Insurance Claims	10 years	Legal requirements	Secure deletion

(7) Unisouk may retain data for requirements under law such as under Income Tax Act, 1961 ('Audit, Assessment and Compliance'), Goods and Services Tax Act, 2017 ('GST Audits, Returns and Input Tax Credit), Companies Act, 2013, Prevention of Money Laundering Act (not applicable for every business) and Regulations / Master Circulars of Securities and Exchange Board of India and Reserve Bank of India etc. In the event due to litigation, investigation, unresolved customer disputes, contractual obligations or request by any government agency, authority etc. DSO to submit a writing request for extension of data retention due to legal reasons, by providing necessary details.

(8) IT to employ best practices of Electronic Data Deletion including 3-pass overwrite on DOD 5220.22-M, cryptographic erasure, certified deletion, physical destruction or certified wiping.

(9) IT to maintain records of deletion, deletion schedules, and verification of successful deletion as per applicable schedules.

(10) DSO to monitor retention policy compliances, ad-hoc, and bi-annually, and internally report any missed deletions. DSO to conduct random checks by sample verification. DSO to monitor quarterly that data classification is done correctly, and data deletion records are properly maintained.

(11) IT to generate Audit Trail of all deletions which have taken place for purposes of Amazon Audit as per DPP.

(12) Customer Order Information and PII only as long as necessary to meet Amazon and tax requirements (e.g., 7 years for invoices).

(13) IT to erase data with certified data destruction equipment when no longer required.

UniSouk - Nexanode Technologies Pvt. Ltd.
601, Solaris Cube, Beside Rajoo India,
Maharana Pratap Road, Vesu,
Surat, Gujarat - 395007.

ACCESS & COMPLIANCE OBLIGATIONS FOR SELLERS

(1) Scope of Seller Data Access

(a) Sellers accessing the Unisouk Platform shall have access strictly limited to:
- (i) Their own order data (including order status, fulfilment details, refunds and returns).
- (ii) Settlement and payment reports relating to their own account.
- (iii) Communication threads with their own customers conducted through Amazon's Seller Messaging system.

(b) Sellers shall not, under any circumstances, access, view, or use:

- (i) Data of any other seller
- (ii) Aggregated or pooled analytics including Amazon Data, unless expressly permitted by Amazon
- (iii) Personally Identifiable Information (PII) or Amazon Data beyond the scope of permitted purposes.

(c) All Amazon Data shall remain logically and technically segregated from other data sources (e.g., ONDC, Website, or Marketing Data).

(2) Seller Compliance Obligations

(a) Sellers agree to process Amazon Data solely for Permitted Purposes, namely: order fulfilment, refunds/returns, customer service, reconciliation, and compliance with applicable laws.

(b) Prohibited Uses include:

- (i) Exporting, merging, or transferring Amazon Data into external CRMs, marketing platforms, or analytics systems.
- (ii) Using Amazon Data for profiling, cross-channel marketing, or enrichment of any non-Amazon database.
- (iii) Sharing Amazon Data with any unauthorized third party.

(c) Sellers shall:
- (i) Maintain unique login credentials, ensure that credentials are not shared, and implement multi-factor authentication (MFA) where provided.
- (ii) Adhere to all applicable laws, the Amazon DPP and Unisouk's IT Policy.
- (iii) Execute an annual Seller Data Handling Attestation confirming adherence to these requirements.

(3) Monitoring & Audit of Seller Compliance

(a) Unisouk shall maintain complete audit logs of all seller activity on the Platform, including access, downloads, and attempted access to Amazon Data.

(b) Unisouk shall conduct quarterly reviews of seller access and activity for anomalies, mass download attempts, or suspicious usage patterns.

(c) Sellers shall fully cooperate with any audit or compliance review conducted by Unisouk or Amazon, including providing records, information, and personnel access as may reasonably be required.

(d) In the event of any breach or suspected breach of these obligations, Unisouk reserves the right to:

(i) Suspend or revoke seller access with immediate effect.

(ii) Report the breach to Amazon and relevant regulators.

(iii) Seek indemnity from the seller for any liability, loss, or claim arising from such breach.

(4) Enforcement

Non-compliance with this Section shall constitute a material breach of the Seller's agreement with Unisouk. Such breach may result in termination of services, legal action, and/or reporting to Amazon in accordance with the Amazon DPP.

INFORMATION SECURITY POLICY

(1) IT shall maintain technical security measures to protect all information assets and ensure confidentiality, integrity, and availability of systems and data. The Access Lifecycle Management, Access Controls, Incident Response, Data Loss Prevention policies shall be an integral part of this Information Security Policy, and the policies are read together.

(2) IT shall ensure Dedicated VLANs are maintained for usage of Amazon resources, with quarterly firewall audits. In the event any vulnerabilities are identified in the Firewall Audits, IT shall ensure that it is rectified within a period of Seven Days, and all access to Amazon shall be suspended until remediation or rectification of vulnerabilities identified in the Firewall Audit.

(3) Information security practices must comply with applicable data protection laws including GDPR, CCPA, and Amazon's Data Protection Policy requirements.

(4) Security controls shall be implemented based on risk assessment outcomes, with higher protection levels for higher classification of information. Highest encryption and strict adherence to deletion requirements shall be maintained in respect of highest classification levels.

(5) Unisouk shall classify information as: Data Classification Levels (i) Level 4: Restricted: Customer Payment Information, Financial Data, HR Employee Records (ii) Level 3: Confidential, Customer order details and personal information, Business strategies and financial plans and Vendor contracts and pricing information (iii) Level 2: Internal: Internal business communications, Operational procedures and policies, Performance metrics and analytics Protection Requirements: User authentication, network controls (ii) Level 1: Public. Marketing materials and public documentation

Data Handling Classification:

Level 4: Restricted	Order information received through Amazon APIs Customer communications via Amazon messaging Return and refund data from Amazon platform, Customer Identity and Payment Details obtained from ONDC / Website Orders, Details of any financial transaction, sensitive legal, compliance or arbitration records.
Level 3: Confidential	Seller Central login credentials, Performance metrics and account health data, Advertising campaign information and spend data, Special Requirements: Multi-factor authentication, access monitoring
Level 2: Internal	Internal Unisouk Operational Knowledge, Procedures, Databases, Internal E-mails, Workflow Documentation, Planning Documentation, Non-Customer Specific API Integration Document
Level 1: Public	Unisouk Website Content, Marketing Material, Published Posts, Advertisements etc.

2) IT shall ensure that for Internal Users authorized to access Amazon API, separate and dedicated service accounts are maintained for that purpose.

3) Amazon API Handling: Separate and dedicated service accounts to be maintained for API Integration, Rotate API key every 90 (Ninety days), Limit Rates for API Calls, Monitor API Calls, Secure Storage of API credentials in approved key management systems.

4) Implement Network Security Best Practices: (i) DMZ for Public-Facing Systems, Separate Network Segments, different data classifications, (ii) Amazon integration systems isolated from general corporate network, (iii) Guest network isolated from business systems Firewall Management Default deny policy for all network traffic, Regular review and cleanup of firewall rules, Change management process for firewall modifications, Logging and monitoring of all blocked and allowed connections Endpoint Security measures: (i) Access Lifecycle Management controls (ii) Endpoint detection and response (EDR) on all devices, Automatic security updates and patch management, Full disk encryption on all laptops and mobile devices

5) Change Management: UniSouk shall maintain a formal Change Management Process to ensure that all modifications to systems, applications, and infrastructure handling Amazon Data are controlled, documented, and reviewed. All proposed changes must be raised through a documented Change Request, clearly outlining the business purpose, potential risks, impact on Amazon Data, rollback procedures, and necessary approvals. No change shall be implemented without prior review and security assessment by the IT Security and Compliance Officers, particularly where changes affect systems storing or processing Amazon PII. Testing of changes shall be carried out only in controlled QA or UAT environments using masked or synthetic data; under no circumstances shall live Amazon Data be used for testing. Deployment into production shall follow a controlled release process, supported by documented rollback plans and version logs. Emergency changes may be implemented only where necessary to maintain

system availability or security, but such changes shall be logged, reviewed, and approved retroactively within twenty-four (24) hours. All changes, whether routine or emergency, shall be logged with details of the individual initiating, approving, and implementing the change, and such logs shall be retained for not less than twelve (12) months and made available to Amazon upon request.

6) Mobile Device Security: Mobile device management (MDM) for business devices, Remote wipe capability for lost or stolen devices, Prohibition of business data on personal cloud storage and Regular security assessment of mobile applications

7) The IT Team Shall regularly conducts scans, tests and screenings to determine and identify any vulnerabilities in the systems, and conduct operating system and application patching within 30 days as per the guidelines mentioned above.

8) IT shall ensure Cloud Security Posture Management (CSPM) tools are deployed, Data is encrypted in transit and at rest, Identity and Access Management Best Practices are implemented and cloud security configurations are regularly reviewed. IT shall implement Server and Infrastructure Security by Server hardening, Cloud Security. Further, all Data accessed by Internal Users shall be at such corresponding level strictly necessary for completion of their roles and responsibilities at Unisouk.

DATA LOSS PREVENTION POLICY

(1) This policy establishes measures to prevent unauthorized access, transfer, or loss of company, customer, and marketplace data, ensuring compliance with Applicable Laws.

(2) Unisouk shall implement / has implemented and is compliant and has duly obtained ISO 270001: 2022 and all cybersecurity best practices, and requirements stated therein are enforced at all material times. All controls shall be implemented in alignment with NIST Cybersecurity Framework where applicable.

(3) Unisouk shall handle data only for lawful basis, legitimate business purpose, with purpose limitations and data minimization. By purpose limitation, Unisouk shall use Amazon Data strictly for order processing, customer support, compliance and operational requirements as per this policy.

(4) Unisouk only collects data which is necessary for performing the functions. Unisouk maintains clear data timeline and particulars for retention of data for performing order fulfilment as contained in Data Retention Policy herein,

(5) DSO shall ensure that all data is maintained using encryption, access control and monitoring to protect against unauthorized use or loss.

(6) IT shall implement and monitor data loss prevention tools, using technical controls such as and including (i) multi factor authentication for all Amazon Seller Central and business accounts (ii) implement rule based access control as per Access Lifecycle Management policy contained herein, (iii) encrypt all data at rest and in transit using TLS 1.2+ and AES-128 with a plan to upgrade to AES-256 in the next six months, (iv) implement endpoint protection through antivirus, device encryption, USB port restrictions, device management, block unauthorized downloads, uploads to external sites, prohibit personal devices (v) key management practices to the standard of AWS KMS or equivalent (v)

content inspection and classification at network boundaries, Email monitoring for sensitive data transmission, cloud application data upload monitoring and (vi) Separate Production and Test Environments (vi) alert generation for potential data exfiltration attempts.

(7) IT shall monitor API data flows and identify unusual patterns. Unisouk to specifically implement rate-limiting and anomaly detection for API usage to prevent data scraping and misuse.

(8) The Legal Department of Unisouk shall incorporate penalties, corrective action, disciplinary actions against Internal Users and End Users in terms and conditions related to their employment to effectively enforce this Policy.

(9) Unisouk has subscribed / shall subscribe to cloud based Data Loss Prevention Solutions to monitor and block unauthorized uploads to external sites. Such cloud based data prevention solutions shall be certified by ISO/IEC 27018, SOC 2 and compliant with Applicable Laws.

(10) IT shall be designated person/ department for reviewing Access Logs on a weekly basis for suspicious activity.

(11) Prohibit sharing of credentials of Amazon Seller Central Login and other Accounts of Unisouk.

(12) Users shall not use public Wi-Fi for business transactions without utilizing Virtual Private Network i.e. VPN, and such VPN shall be that which is authorized by Unisouk's IT Department and informed to Internal Users to be used in that regard.

(13) IT shall enforce policy of strict use of only Unisouk provided devices for any operations of Unisouk.

(14) All Internal Users shall remain up-to-date on Employee Trainings as per the Employee Awareness and Training Section of this Policy.

(15) All Third-Party Vendors accessing Restricted / Confidential data must consent to Terms and Conditions / EULA / Data Protection Agreement.

THIRD-PARTY VENDOR COMPLIANCE POLICY

(1) Pre-Approval of Vendors
- (a) No third-party vendor, subcontractor, or service provider shall be engaged to access, process, or store Amazon Data without:
  - (i) Written approval of the Data Security Officer (DSO), and
  - (ii) Where required, written approval from Amazon in accordance with the Amazon DPP.
- (b) Unisouk shall maintain a central register of all approved vendors with access to Amazon Data, including scope of services, date of approval, and contract status.

(2) Mandatory Contractual Safeguards

All vendor contracts involving access to Amazon Data must include, at a minimum:

(a) Data Processing Agreement (DPA) aligned with Amazon DPP standards.
(b) Audit Rights in favor of Unisouk and Amazon, permitting both scheduled and ad hoc inspections of systems, facilities, personnel, and policies.
(c) Breach Notification obligation requiring written notice to Unisouk within 24 hours of discovery of any suspected or actual breach, incident, or unauthorized access to Amazon Data.
(d) DPP-Aligned Privacy Terms requiring strict data minimization, purpose limitation, segregation of Amazon Data, encryption in transit and at rest, and prohibition of secondary uses.
(e) Subcontracting Restrictions, requiring prior written consent from Unisouk (and Amazon where applicable) before engaging any sub-processor.

(3) Vendor Compliance Obligations

(a) Vendors must maintain technical and organizational safeguards equivalent to those mandated for Unisouk under this Policy, including MFA, encryption, and role-based access controls
(b) Vendors shall provide annual written attestations of compliance with the Amazon DPP and this Policy.
(c) Vendors must ensure that any employees handling Amazon Data complete mandatory security and Amazon DPP training prior to being granted access, and annually thereafter.
(d) Vendors shall immediately cooperate with Unisouk and Amazon during any audit, compliance review, or investigation.

(4) Monitoring and Enforcement

(a) Unisouk shall conduct annual vendor assessments to verify compliance with this Policy, including security testing, review of audit logs, and validation of deletion practices.
(b) Non-compliance by any vendor shall result in suspension or termination of access, and may be reported to Amazon in accordance with the Amazon DPP.
(c) Vendors shall indemnify and hold Unisouk harmless against any liability, loss, or claim arising from their breach of the Amazon DPP or this Policy.

AUDIT PREPAREDNESS POLICY

(1) Amazon, or its designated third-party auditor, shall have the right, upon reasonable prior notice, to conduct audits, inspections, or examinations of the Data Fiduciary's (and its Subcontractors', where applicable) facilities, systems, processes, policies, records, and personnel relevant to the processing of Amazon Data, in order to verify compliance with the Amazon DPP and any applicable data protection laws. Such audits may include on-site inspections, remote assessments, and review of documentation.

(2) Unisouk shall:

(a) Provide full cooperation, access, and assistance to Amazon or its auditors, including access to relevant premises, personnel, systems, and records.

(b) Promptly implement reasonable corrective measures identified by Amazon as necessary to remedy any material non-compliance.

(c) Ensure that its Subcontractors agree to equivalent audit rights in favor of Amazon.

(d) Bear its own costs of cooperation, provided that Amazon shall bear the costs of any third-party auditor it engages.

(e) Amazon shall exercise its audit rights in a manner designed to minimize disruption to Unisouk's business operations.

(3) The Company is at all times prepared for any audits by Amazon regarding compliance with Amazon DPP and all applicable data protection policies, terms and conditions and contracts.

(4) Unisouk logs Order Fulfillment Date by Auto Logging and Deletion Date for Audit purposes.

(5) Unisouk to ensure HR maintains complete log with particulars of the training of Internal Users as per this Policy.

(6) Unisouk has obtained express indemnity and undertaking from its Customers for complete co-operation with Unisouk and Amazon for the purposes of Audits.

(7) Unisouk shall conduct an internal audit of its systems every six months in order to verify compliance with the Amazon DPP and any applicable data protection laws.

EMPLOYEE AWARENESS AND TRAINING

(1) Users must complete Amazon DPP training before first login.

(2) All Internal Users who are members of Incident Response Team as per Incident Response Policy hereinabove shall receive annual incident response training or when there are updates to (i) data protection laws, (ii) Amazon DPP (iii) DPP of any other third parties relevant to Unisouk and other material developments relevant to the IT Policy of Unisouk.

(3) All Internal Users interacting with Amazon Data, PII or Environment shall receive training in Amazon specific best practices, Amazon security policies and procedures, customer data handling requirements, seller central security features, API security best practices, process improvements etc. once every year.

(4) All Internal Users shall general receive training viz.,(i) 'Annual Security Awareness Training' (ii) incident awareness and reporting training (iii) data protection training once every year (iv) training on Remote access best practices, Wi-Fi Use, etc.. Tabletop exercises, discussions, simulations etc. shall be part of such training.

(5) All Internal Users who are also IT Personnel shall receive role-specific security training, be trained in cloud security, secure coding, and incident response procedure.

(6) IT shall circulate e-mails of phishing and data security best practices regularly, and Users shall read and understand such e-mails.

(7) IT shall conduct randomized phishing, security, other tests on Users to ensure employee awareness and preparedness, and provide corrective training to Users as necessary.

(8) IT to develop training modules and maintain the same for easy access to Internal Users for their training as and when may be necessary.

(9) HR to track completion of training as part of employee related compliances and maintain details of training undergone by Internal Users.