Supplier & Purchasing Agreement Policy

Netwealth Group Limited

ABN 84 620 145 404

Level 6, 180 Flinders Street
Melbourne VIC 3000

PO Box 336
South Melbourne VIC 3205

Netwealth Group Limited

Approved and adopted by:

- Netwealth Investments Limited (NIL) (ABN 85 090 569 109) AFSL (230975) (in the capacity of RE and Operator) on 27 October 2021
- Netwealth Group Limited (ABN 84 620 145 404) on 27 October 2021
- Netwealth Holdings Limited (ABN 57 133 790 146) on 27 October 2021
- Netwealth Group Services (ABN 89 135 940 840) on 27 October 2021
- Netwealth Superannuation Services (ABN 80 636 951 310) AFSL (528032) RSE Licence (L0003483) on *TBC*

Document classification: General use

Document version control:

Document owner	Risk and Compliance
Frequency of Review	Biannually
Date of next scheduled review	October 2023
Regulator	ASIC, APRA
Legislative framework	▪ RG104 – Licensing: Meeting the general obligations ▪ NIL AFSL conditions ▪ Privacy Act 1988 and Australian Privacy Principles ▪ AML/CTF Act & Rules ▪ CPS234 Information Security (Jul 2019) ▪ Modern Slavery Act 2018 (Cth)

1.0 Document overview

1.1 About the document

Netwealth Group Limited and its subsidiaries (**Netwealth)** are committed to promoting and supporting the creation of ethical supply chains. The Supplier and Purchasing Agreement Policy (**the Policy**) is applicable to each of the Netwealth entities who have formally adopted the Policy (as detailed on the cover of the Policy) and is designed to assist Netwealth in choosing and managing new and existing Supplier and Purchasing Agreements.

This Policy covers the responsibilities when entering into a Supplier or Purchasing Agreements, the Supplier and Purchasing Framework (including Risk Assessment) and the ongoing monitoring of Suppliers.

Note:

- For Netwealth Superannuation Services Pty Ltd (ABN 80 636 951 310) (**NSS**), this Policy is to be read in conjunction with the NSS Outsourcing and Supplier Management Policy, which outlines NSS's obligations relating to the management of Material Outsourced Arrangements.
- This Policy does not apply to Investment Manager arrangements between Netwealth Investments Limited (**NIL**) (as Responsible Entity) and the Investment Manager. These arrangements are covered by the Managed Investment Schemes Managed Account – Investment Management Policy and are monitored by the NIL Investment Committee.
- Where NIL is the Responsible Entity and have Managed Investment Schemes (MIS), the appointment of Suppliers may be required to assist with the administration and custodian of certain MIS products. This appointment is covered by this Policy and is different to the appointment of Investment Managers.

1.2 Roles and responsibilities

The following table sets out the roles and responsibilities for those involved in implementing and monitoring the Policy.

Role	Responsibilities
NGL Board	• Delegate ongoing approval and monitoring of this Policy to the CRMC • Approve the annual Modern Slavery Statement • Oversee new Supplier Agreements (through Sealings)
Compliance Risk Management Committee (**CRMC**)	• Approve the Policy for all Netwealth entities (except NSS) • Oversee the management and monitoring of Supplier agreements and compliance with the Policy • Report risks and issues to the Board as applicable
Audit Risk and Compliance Committee (**ARCC**)	• Approve the Policy for NSS • Report risks and issues to the Board as applicable
Netwealth Investments Ltd Executive Team	• Oversee Supplier agreements on a day-to-day basis and ensure that appropriate procedures, processes, reporting, and controls are in place

Role	Responsibilities
(**Management**) / Office of the Trustee (**OTT**)	• Provide approval and individual accountability for all new Supplier agreements that are executed within their business area
Business Owner	• Complete the Supplier Management Checklist using the Supplier & Purchasing Agreement Process Guide, and provide a copy of the completed Checklist and executed contract to sealings@netwealth.com.au **(Sealings)** • As necessary, provide contracts pre-execution to Legal for review • Oversee and manage Supplier arrangements, including ensuring that requirements under the contract are performed (including SLA compliance and reporting) • Escalate quality issues and/or non-performance issues in relation to a Supplier arrangement to the Governance Manager (and if applicable the CRMC / ARCC) • Review and provide updates to Sealings on contracts • Disclose any Conflicts of Interest arising at any stage of a Supplier assessment, such as an Employee having a personal relationship with a Supplier or where an Employee is offered a reward for engaging a Supplier
Governance Team	• Identify, assess, manage, mitigate, and report on risks associated with Supplier arrangements, including undertaking risk assessments • Work with the OTT on new supplier arrangements that may be material for NSS to ensure the OTT are able to meet the requirements of the NSS Supplier and Outsourcing Policy • Maintain appropriate controls in Protecht to support and monitor compliance with the Policy • Maintain a Supplier Register, detailing all Supplier Agreements • Support the business in managing their Supplier arrangements • Owner of and responsible for filing executed contracts (electronically and/or hard copy, as applicable) • Complete the annual Modern Slavery Statement • Conduct training on the Policy for all employees
IT Risk Team	• Work alongside the Governance Team to review all new and ongoing Supplier agreements where the Supplier has access to Personal Information Data, including assessment of any security operational control reports (as necessary), penetration tests (as necessary) and IT Risk Questionnaires to ensure the Supplier has appropriate information security controls in place commensurate with the criticality and sensitivity of the data they have access to.
Legal	• Review new supplier contracts as requested
Internal Auditor	• Review this Policy from time to time as determined by the NGL Audit Committee.

1.3 Definitions

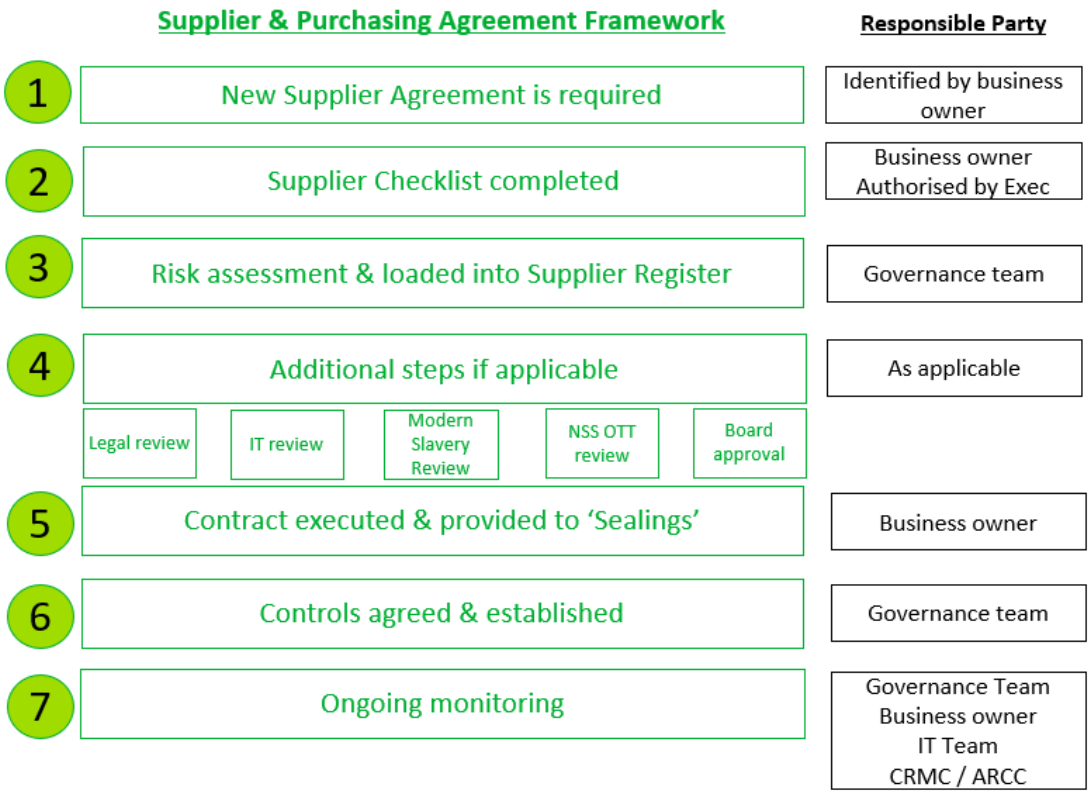
Term	Definition
Board	The Board of Netwealth Group Limited.
Business Owner	Nominated employee who is responsible for the oversight and management of a Purchasing or Supplier Agreement.
Conflict of Interest	Defined in the Conflicts Management Policy.
Employee	An individual employed by Netwealth Group Services Pty Ltd (ABN 89 135 940 840).
Goods	Physical, material, and tangible property.
Inherent Risk Rating	The natural level of risk inherent in a process or activity before risk mitigation treatment has been applied.
Intellectual Property	Intangible property created by Netwealth.
Material Outsourced Arrangement	Defined in the NSS Outsourcing & Supplier Management Policy.
Modern Slavery	Contemporary form of slavery where offenders exploit victims and undermine their freedom.
Netwealth	The Netwealth Group including the entities detailed on the cover of the Policy.
OTT	Office of the Trustee, Netwealth Superannuation Services Pty Ltd.
Overseas Supplier	A Supplier based outside of Australia.
Personal Identifiable Information Data (PII Data)	Any information related to an identifiable person.
Protecht	The Risk Management Software used by Netwealth.
Purchasing Agreement	A one-off purchase of either goods or services which is unlikely to be ongoing and does not usually require a written contract.
Services	Activities which are offered by a Third-Party without transferring the ownership of a product.
Supplier	A third party who suppliers a Good or Service to Netwealth.
Supplier Agreement	Engagement of a party to supply goods and/or services which is likely to be on-going and usually requires a written contract.
Supplier Checklist	An internal document to be completed by the Business Owner seeking to enter into a new or renewed Supplier or Purchasing Agreement.
Supplier Register	An internal register maintained by the Risk & Supplier Analyst, which keeps record of all Purchasing and Supplier Agreements for Netwealth.
Supply Chain	The network which allows for the flow of Goods and Services to be produced and distributed between businesses.
Third-Party	A person or group outside of Netwealth.

2.0 Board expectations

The Board expects its Suppliers to behave ethically, apply high standards of corporate conduct and to fully comply with all relevant laws. When considering, entering, managing, and monitoring Purchasing and Supplier Agreements, the Board expects Management and Business Owners to balance the achievement of outstanding performance and value for money with risk considerations, such as consideration of data security, IT security and modern slavery.

3.0 Supplier and Purchasing Agreement framework

When entering a new or renewed Supplier or Purchasing Agreement, the below framework should be followed:



3.1 Supplier agreement required

It is the responsibility of each Business Owner, in conjunction with the relevant member of the Executive team, to determine the business need for the new or renewed Supplier or Purchasing Agreement.

3.2 Supplier Checklist

Each Business Owner will complete the Supplier Checklist when they wish to enter into a new or renewed Agreement. The Checklist has been designed to make the process of establishing a new or renewed Supplier or Purchasing Agreement within the business efficient and effective. The Checklist will take the Business Owner through the process of onboarding the Supplier and will prompt them where there are additional steps required based upon the nature of their Agreement, such as legal or IT review.

3.3 Supplier risk assessment

Once the Business Owner has completed the Supplier Checklist, the Governance Team is responsible for collating the information from the completed Checklists into the Supplier Register and using this information to undertake a risk assessment of any new Supplier in accordance with the NIL/NSS Risk Management Strategy and the processes established for Supplier Risk Assessment.

Netwealth recognises that a robust risk assessment framework of its Supply Chains is required to minimise potential risk and avoid disruption to the business. The Risk Assessment Methodology and the explanations of Risk Consequence and Risk Likelihood used by Netwealth are outlined in the NIL/NSS Risk Management Strategy.

The risk rating of a Supplier is calculated by reference to three categories of risk. Information relating to each of these three areas is to be provided by the Business Owner on the Supplier Checklist, including:

- General Risk – including whether a Supplier has access to Netwealth's internal systems or whether the Agreement will involve the Netwealth Superannuation Master Fund, a service to the Fund or use of the Fund's data;
- IT Risk – including whether a vendor has access to PII Data for clients, staff or Netwealth Superannuation Master Fund members; and
- Modern Slavery Risk – including the Supplier's country of origination, whether the Supplier has a modern slavery statement or not and the type of goods and services being provided by the Supplier.

The answers provided to each of the three categories of risk determine the level of risk associated with that category as either low, medium, high or extreme risk. These are then collated, and the inherent risk rating of the Supplier is calculated as either low, medium, high or extreme as per Appendix 1.

3.4 Additional steps if applicable

The answers provided by the Business Owner will establish additional steps required, such as a:

- Legal review – required when:
  a) Netwealth is signing the agreement template of an external party and the Executive owner feels that this is necessary.

b) The Supplier has access to client data or Netwealth's intellectual property.
c) The arrangement involves a spend of more than $100k in the next 12 months or has an ongoing liability of more than $100k in the next 3 years.
d) There are significant changes, that the Executive is not able to approve, to a Netwealth template Agreement.

- IT review – required when a supplier has access to PII data, as defined in the Data Governance Policy.

- Modern Slavery review – required when the Supplier:
  a) Is located in a medium or high-risk country.
  b) Is providing higher risk goods or services.
  c) Has a higher risk business model or routinely employs migrant or base-skill workers.

- OTT review - required when the Supplier Agreement is considered a Material Outsourced Arrangement under the NSS Outsourcing & Supplier Management Policy.

- Board approval – required for all extreme risk rated Suppliers.

3.5 Contract execution

The Business Owner is then informed of the inherent risk rating of the Supplier by the Governance Team and advised whether contract execution can proceed and, if so, what requirements must be met before proceeding based upon the inherent risk-rating of the Supplier. The Business Owner is responsible for executing the Agreement and providing a copy of all executed Agreements to the Governance Team at sealings@netwealth.com.au.

In all cases (regardless of risk rating) if the Agreement is a Material Outsourced Arrangement, then evidence is required that the NSS Supplier and Outsourcing Management Policy has been followed, including due diligence, an internal audit review and NSS Board approval. This evidence is to be provided to the Governance Team.

The following steps should be taken when executing an Agreement with Suppliers based upon their risk rating:

Extreme Risk Rated Suppliers

A paper seeking Board approval is required, which should explain why the Supplier has an extreme risk-rating,
the risks associated with the arrangement and provide information and evidence of the following:

- If the Supplier has access to critical and/or sensitive PII data - A penetration test (as applicable to the arrangement) and a security operational control report (SOC), both of which have been assessed by the IT Risk team and approved;
- Evidence that the Supplier and its owners have been appropriately screened in accordance with the AML Program;
- Any controls that have been agreed to monitor the arrangement or to mitigate the associated risks; and
- Approval by the Executive or Joint Managing Directors of the arrangement.

High Risk Rated Suppliers

- If the Supplier has access to critical and/or sensitive PII data - a penetration test (as applicable to the arrangement) and a security operational control report (SOC), both of which have been assessed by the IT Risk team and approved;
- Evidence that the Supplier and its owners have been appropriately screened in accordance with the AML Program;
- Appropriate controls should be agreed and established by the Governance Team and the Business Owner to mitigate risk; and
- Approval of the contract by Directors / Company Secretary, or an authorised signatory in accordance with the Board Delegation Policy

Medium Risk Rated Suppliers

- If the Supplier has access to critical and/or sensitive PII data - a penetration test (as applicable to the arrangement) and a security operational control report (SOC), both of which have been assessed by the IT Risk team and approved; and
- Approval of the contract by Directors / Company Secretary, or an authorised signatory in accordance with the Board Delegation Policy

Low Risk Rated Suppliers

- Approval of the contract by an Executive or Senior Manager as defined in the Board Delegation Policy.

3.6 Controls agreed and established

Where the inherent risk rating of a Supplier is calculated to be high or extreme, appropriate controls should be agreed and established by the Governance Team and the Business Owner to effectively mitigate risk associated with the Agreement. These controls are to be recorded and maintained in Protecht by the Governance Team.

Where controls are deemed necessary, a residual risk rating will be assigned to each Supplier based upon the effectiveness of those controls.

3.7 Ongoing monitoring

The ongoing monitoring requirements of a Supplier is dependent upon either the inherent risk rating of the Supplier (where no controls are necessary) or the residual risk rating of the Supplier (where controls have been agreed and established).

Note: for the purpose of the below section the Business Owner can also refer to their Executive Manager, and Governance Manager can refer to the Governance Manager or their Executive Manager.

In all cases (regardless of risk rating) if the Agreement is a Material Outsourced Arrangement, then evidence that the NSS Supplier and Outsourcing Management Policy monitoring has occurred should be provided to the Governance Team.

Extreme Risk-Rated Suppliers

- Quarterly review meetings with the Business Owner or delegate;
- Annual review including questionnaire and site visit (including the Business Owner and Governance Manager), with the results provided to the CRMC and/or ARCC as applicable;
- Annual review of the Supplier's risk assessment rating; and

- Annual review of the Supplier's SOC report and biannual penetration test conducted by IT Risk Team (where Supplier has access to critical and/or sensitive PII data).

High Risk Rated Suppliers

- Annual review meetings with the Business Owner and Governance Manager;
- Annual review of the Supplier's SOC report and a penetration test every 3-5 years conducted by IT Risk Team (where Supplier has access to critical and/or sensitive PII data); and
- Annual review of the Supplier's risk assessment rating.

Medium Risk Rated Suppliers

- Annual review meetings with the Business Owner; and
- 3-year review of the Supplier Arrangement and Risk Rating by Governance Team.

Low Risk Rated Suppliers

- No ongoing monitoring requirements needed.

The remediation process for issues that have been identified within the ongoing management of Suppliers is dependent upon both what type of issue has been identified and the role of the Supplier.

Netwealth has a low-risk tolerance for any issues identified in relation to Suppliers who have access to critical and/or sensitive PII data, so Netwealth will cease to engage such a Supplier if they fail to provide an adequate SOC report or do not commit to and remediate findings from a penetration test within a reasonable period.

If an issue is identified in relation to an extreme or high risk rated Supplier, the CRMC/ARCC (as relevant) must be notified and appropriate remediation must be sought if applicable or, if remediation is not possible or is protracted, a proposal to cease the Arrangement should be provided.

If issues are identified in relation to the ongoing monitoring of performance against SLA's, this is to be actioned appropriately as determined by the Business Owner responsible for the Supplier relationship.

4.0 Board, CRMC and ARCC Reporting

Any proposal to enter a new or to renew a Supplier Arrangement should be prepared by the Business Owner and their Executive by following the Supplier Checklist.

Where Board approval is required, the Business Owner should work with the Governance Team on how to meet the requirements of this policy and what is required for the Board Report. The Governance Team will arrange for the Supplier Arrangement proposal and any applicable attachments to be provided to the Board and will advise the Business Owner of approval or otherwise.

A quarterly report to the CRMC and the ARCC will be provided by the Governance Manager. This will provide a summary of any key activity for the period in relation to Supplier Arrangements and will provide a summary of the extreme and high-risk Suppliers, outcomes of annual reviews and reassessments and any material changes to risk.

5.0 Amendment and approval

This Policy will be reviewed biannually or more frequently as required to ensure it remains appropriate with regard to the changing nature of legislation, regulations and Netwealth's operations. Compliance with this Policy will be monitored by the Governance Team.

Ongoing approval of the Policy has been delegated to the CRMC and the ARCC.

Appendix 1 – Supplier risk assessment methodology

5.1 Supplier risk assessment framework

The following provides an overview of the categories of risk that are considered by the Governance Team as part of the Supplier risk assessment:

General Risk:

1. Does the Supplier have access to Netwealth's internal systems?
   - Yes = medium risk, No = low risk
2. Does the Supplier have access to Netwealth's internal systems that include PII?
   - Yes = high risk, No = low risk
3. Is the Agreement a Material Outsourced Arrangement (i.e. Critical for CPS234)
   - Yes = high risk, No = low risk

IT Risk:

1. Does the Supplier have access to any PII data?
   - Yes = see below, No = low risk
     a. Medium risk = the Supplier has access to employee, non-superannuation member or superannuation member classified as low sensitivity in the Data Governance Policy
     b. High risk = the Supplier has access to employee, non-superannuation member or superannuation member data rated as medium sensitivity in the Data Governance Policy

c. Extreme risk = the Supplier has access to employee, non-superannuation member or superannuation member data classified as high sensitivity in the Data Governance Policy

Modern Slavery Risk:

1. Can the Supplier provide any evidence of ethical procurement policies/a Modern Slavery statement?
   Yes = low risk, No = See below
2. Where is the Supplier located?
   - Australia and other low-risk countries (e.g. UK, USA) = low risk
   - Mid-risk countries (e.g. Russia, Thailand, Indonesia) = medium risk
   - High-risk countries (e.g. China, North Korea, Pakistan, Cambodia) = high risk
3. What type of goods and/or services is the Supplier providing?
   - High risk goods./services (e.g. textiles, hospitality, cleaning) = medium risk
   - Low risk goods/services (e.g. marketing, consulting, software) = low risk
4. What type of business model does the Supplier have?
   - High risk business model (e.g. labour hire, outsourcing and franchising) = medium risk
   - Low risk business model = low risk
5. Does the Supplier regularly engage with base-skill workers (e.g. hospitality, cleaning, textiles, farming)?
   Yes = medium risk, No = low risk

5.2 Calculating the inherent risk rating of a Supplier

Once the risk assessment has been undertaken based upon the information provided in the Supplier Checklist, the overall inherent risk rating of a Supplier is to be calculated by the Governance Team as follows:

	1 Extreme	1 High	1 Medium	Lows
PLUS				
1 Extreme	Extreme	Extreme	High	Medium
1 High	Extreme	High	Medium	Low
1 Medium	High	Medium	Medium	Low
Low	Medium	Low	Low	Low