REQUEST FOR TENDER

Payroll and Timesheet System Services

RFT 2022-2023 003

The Australia Council for the Arts (Australia Council) is the Australian Government's principal arts investment, development and advisory body. We are currently seeking the services of a payroll and timesheet provider. The successful provider will include a payroll and timesheet system for the completion of in-house processing.

This document is available until the closing date.

Issue Date: 11 January 2023

Tender Closing Time: 9 February 2023, 10:00am AEDT

Lodgement Address: tenders@australiacouncil.gov.au

LODGEMENT OF TENDERS

Applications should be sent by a secure email and received **by 10am local Sydney, NSW time on 9 February 2023**. The application should be endorsed with the above reference number and title addressed as follows: **Payroll and Timesheet System Services RFT 2022-2023 003.**

By email to: **tenders@australiacouncil.gov.au**
Include email subject line: Payroll and Timesheet System Services RFT 2022-2023 003

Applicants are to submit an original application and any supporting material by the due date; late applications will not be accepted.

HAND OR POSTAL DELIVERY **will not** be accepted

FAXED APPLICATIONS **will not** be accepted.

All enquiries in relation to this Request for Tender are to be emailed in the first instance.

Contact details:

Steve Wong, Human Resources Manager

Email: tenders@australiacouncil.gov.au

Applicants are required to check the Australia Council website for any additional information which may be published while this RFT is open.

PART A – CONDITIONS FOR PARTICIPATION

A1. INVITATION

Tenderers are invited to make an offer (**Tender**) that meets the requirements of this Request for Tender (**RFT**).

This RFT is expressly not a contract between the Australia Council and the Tenderer. Nothing in this RFT or in any tender is to be construed as to give rise to any contractual obligations, express or implied.

We reserve the right to stop or vary the tender process, determine a shortlist of Tenderers, negotiate or decline to negotiate with any Tenderer, negotiate with more than one Tenderer, or re-tender, at any time. We are not bound to accept the lowest priced tender or any tender.

If we make a variation to the original RFT, we will take all reasonable efforts to ensure that the Addenda or supplement is given the same distribution as the original RFT.

A2. ENQUIRIES BY TENDERERS

All enquiries by potential tenderers should be made via email in the first instance.

A3. LODGEMENT OF TENDERS

Tenders must be lodged by the Tender Closing Time shown on the cover page of this RFT. Before lodgement of tenders, the Tenderer must initial any alterations or erasures made to a tender. Late tenders will not be accepted.

A4. OWNERSHIP OF TENDER DOCUMENTS

All tender documents become the property of the Australia Council on lodgement.

A5. NON-COMPLIANCE

Any non-compliant tenders may be excluded from consideration.

A6. TENDERERS TO MEET COSTS

Tenderers are to meet all costs of responding to this RFT, including preparation, submission, lodgement and negotiation costs.

A7. TENDERERS TO INFORM THEMSELVES

Tenderers are considered to have:

(a) examined the RFT and any documents referred to in the RFT as being available;

(b) satisfied themselves as to the correctness and sufficiency of their tenders including tendered prices.

Each part of this tender must be satisfactorily completed by the Tenderer at the sole discretion of the Australia Council. Where a part of this tender is not satisfactorily completed, the Australia Council will reserve the right to exclude the tender from further consideration.

A8. IMPROPER ASSISTANCE AND COLLUSIVE TENDERING

It should be noted that the Australia Council shall exclude from further consideration, tenders which have been compiled:

(a) with improper assistance of employees, ex-employees, any consultant or adviser to the Australia Council; or

(b) in collusion with other Tenderers.

A9. DRAFT GENERAL TERMS AND CONDITIONS OF CONTRACT

Draft general terms and conditions of contract are attached to this RFT. These draft contract terms and conditions are intended to form the basis of any contract between a successful Tenderer and the Australia Council.

Tenderers please note, the Tenderer is taken to agree to accept these Draft Terms and Conditions of Contract.

A10. CONFLICT OF INTEREST

You must declare any actual or perceived conflict of interest that is likely to arise if your submission is the successful tender and how this conflict is proposed to be managed. Where, in the opinion of the Australia Council, the conflict of interest is one that compromises the integrity of the tender process and is unlikely to be able to be satisfactorily managed, the Australia Council reserves the right to treat your submission as unsuccessful.

A11. PROCUREMENT TIMETABLE

It is proposed that the following procurement timetable shall apply. We will strive to adhere to this timetable but reserve the right to vary dates whenever necessary.

Date	**Activity**
11/01/2023	Request for Tender published
09/02/2023	Request for Tender closes
Week commencing 13/02/2023	Submitted Tenders acknowledged Eligibility checked
Week commencing 13/02/2023	Tenders evaluated by the Tender Evaluation Committee (TEC)

Between 27/02/2023 and 28/02/2023	Shortlisted Tenderers will be contacted to provide a system demonstration
Week commencing 27/02/2023	Successful tender notified and contract issued Contract executed by both parties
Week commencing 06/03/2023	Unsuccessful tenderers notified
13/03/2023	Work to commence

Where this timetable varies significantly, we will attempt to notify prospective Tenderers as soon as is practicable.

A12. SECURITY, PROBITY AND FINANCIAL CHECKS

We may, as part of the evaluation process, conduct such security, financial or probity checks as we consider necessary in relation to any Tenderer, its officers, employees, partners, related entities and nominated subcontractors.

Tenderers will be expected to provide reasonable assistance to us regarding such checks, including supplying further information as we may request.

Any failure by a Tenderer to assist us in conducting these checks may have an adverse impact upon the evaluation of the affected tender.

A13. NOTIFICATION

All Tenderers will be informed in writing of the outcome of their submission at the earliest opportunity.

A14. CONFIDENTIALITY OF TENDERER'S INFORMATION

Tenderers should note that if successful, parts of their response may be included in a subsequent contract. Tenderers must identify any aspects of their response or the proposed contract that they consider should be kept confidential, including reasons.

Tenderers should note that the Australia Council will only agree to treat information as confidential in cases that it considers appropriate. In the absence of such an agreement, Tenderers acknowledge that the Australia Council has the right to publicly disclose the information.

A15. TENDER DOCUMENTS

Tenderers are required to submit a total of four (4) documents in response to this RFT as follows:

1. Payroll and Timesheet System Vendor Response (maximum 20 pages) to include the following:

    - A Description of the tenderers proposed payroll and timesheet system, addressing the Council's requirements as outlined under Part B – Statement of Requirements.
    - A breakdown of the total cost of the proposal, inclusive of the contract's five (5) year potential and any scheduled price increases during the term, with detailed costing identifying the items or services proposed, including and noting GST where applicable.
    - If travel will be involved this should also be itemised and costed.
    - Company or organisation information such as corporate status, registered place of business, size, number of staff & turnover, and copies of financial statements demonstrating financial viability and insurance policies.
    - Supporting information concerning the proposing organisation, its management structures and procedures, quality assurance procedures and demonstrated experience in the subject area of this RFT and related areas.
    - A risk analysis, setting out perceived potential risks, the level of potential impact of such risks and the contingencies to mitigate any potential damage resulting from such risks.
    - Two referees to whom the Australia Council may address enquiries concerning previous experience in this area.
    - A declaration of any partial or non-compliance with any provisions of this RFT. This includes not agreeing to any of the draft conditions of contract stating reasons and alternatives where appropriate.

2. Payroll and Timesheet System and Module Functionality Questionnaire (attached separately)

3. Payroll and Timesheet System IT Security Questionnaire (attached separately)

4. IT Service Questionnaire (attached separately)

PART B – STATEMENT OF REQUIREMENTS

B1. REQUIREMENT

The Australia Council requires the services of a company to provide a cloud-based (SaaS) payroll and timesheet system. The Australia Council will complete the payroll processing in-house.

The contract will have a potential five (5) year term and will be for an initial period of three (3) years with the option of two (2), one (1) year extensions exercisable at the sole discretion of the Australia Council.

Tenderers must be able to demonstrate that they have the necessary skills, resources, experience, financial capacity and relevant licenses, accreditations etc to fulfil the tender requirements.

B2. FURTHER DETAILS

The Australia Council is seeking tenders to provide a complete payroll and timesheet system. The Australia Council would manage the payroll and timesheet process (eg not outsourced payroll completion services).

The Australia Council is a federal government agency with a payroll of up to approximately 150 employees (including the Australia Council board). Tenderers should include a cost estimate should the Council experience a period of growth.

Employees are either covered by the Australia Council Enterprise Agreement 2017-2020 or employed under a common law contract.

B3. SCOPE OF WORKS

General

It is expected that works are fully completed and transitioned to the new payroll system to align with the Council's first pay run of the 2023-24 financial year, being 5 July 2023.

The tenderer must submit any additional contractual terms that are not outlined in Part C, if required and for the Australia Council's consideration.

The successful payroll and timesheet system will be intuitive for users and easily configurable for administrators. The system will have detailed and customisable administrator reporting functionality.

1. Payroll module

Delivery of a **payroll module** configured to meet the Australia Council's legislative and reporting requirements. The payroll system will enable the Australia Council to complete its fortnightly payroll processes and related reporting requirements to the Australian Tax Office (ATO) and superannuation. This includes but is not limited to:

- Compliance reporting through Single Touch Payroll (STP)
- Tax updates available for system implementation by service provider on request from the Australia Council to comply with Australian Tax Office (ATO) rulings

- SBR registered system that can upload Tax File Number (TFN) declarations directly to the ATO. If the payroll provider is STP Phase 2 compliant then this is not required
- Production of fortnightly payslips for employees to view and download

Superannuation

The payroll system must be able to meet the superannuation requirements of government superannuation funds in addition to APRA regulated and self-managed super funds. This would be through a direct submission to the funds or through a clearing house.

The payroll system will also need to have the functionality to:

- Create a SAFFE file for Superstream compliance with the Government's superannuation funds:
    - Public Sector Superannuation defined benefits (PSSdb)
    - Commonwealth Sector Superannuation defined benefits (CSSdb)
    - Public Sector Superannuation accumulation plan (PSSap)

The PSSdb, CSSdb and PSSap superannuation plans have additional reporting requirements, and the payroll system must be able to comply with them.

The system will also have the capability of facilitating salary sacrifice arrangements for individuals in the system.

The payroll module will facilitate accurate leave accruals based on applicable legislation staff are covered under, being:

- Long Service Leave (Commonwealth Employees) Act 1976
- Maternity Leave (Commonwealth Employees) Act 1973
- Australia Council Enterprise Agreement 2017-2020

2. Timesheet module

Delivery of a **timesheet module** configured to meet the requirements as set out in the Australia Council Enterprise Agreement 2017-2020.

The Australia Council requires a timesheet system to track work credit accruals and debits (time worked / not worked) for staff classified in Bands 1-4 under the Australia Council Enterprise Agreement 2017-2020.

All employees are on autopay and the hours worked/not worked is not linked to pay rates, rather the accrual of work credits.

Under the Enterprise Agreement, the standard working day for a full-time employee is 7 hours and 21 minutes, excluding breaks. The timesheet system will track any minutes and hours an employee works above/below this standard day. With manager approval a full-time employee may accrue a maximum of:

- 37.5 hours work credits (pro rata for part-time employees), and
- 29.4 hours work credit bank (pro rata for part-time employees), which are transferred from work credits into the bank on an employee request

The work credit system is in place to provide flexibility to staff to commence /finish work at times agreed between them and their manager (and must be between 7:30am to 7:00pm). Where an employee works additional hours, they can use work credits flexibly by working fewer hours in a day – the ebb and flow of time against the peaks and troughs of operation requirements. In addition, full or part days can be applied for as a substitute for other leave types.

The timesheet also needs to:

1. Capture when an employee logs in and out
    a. Does not allow an employee to log in prior to 7:30am or after 7:00pm or on a non-working day
    b. Work patterns and daily hours are customisable to meet individual circumstances and agreements in working hours and days
2. Provide the ability for the employee to edit log in/out times as well as their break length
3. Calculate the work credit accrued/debited on a daily basis based on the hours worked, less breaks
4. Manager ability to approve and/or modify daily timesheet records for their employees
5. Work credit accruals are only available for the employee to use on manager approval
6. Work credit accrual cap applies when a full-time employee reaches their maximum approved hours of 37.5, and pro rata for a part-time employee

3. Employee Self Service module

The payroll and timesheet system will provide an **employee self-service** (ESS) portal through single sign-on. In the ESS portal employees will be able to view their:

- position history
- remuneration details
- payslips

Employees will have the ability to update:

- home address and emergency contact details
- bank account details (with an audit trail and email notification confirming to the employee and payroll administrators of the changes made)

Employees will also apply for leave (i.e. annual, personal, work credit, etc) in the system with system generated emails being sent to managers for approval.

Managers in the ESS portal should have a dashboard which shows their teams leave balances. Managers would also approve leave requests in the ESS portal.

IT Requirements

It is expected that the tenderer will account for the cost of completing at least 2 instances of data migration from the current payroll system and the current timesheet system to the new payroll system. The 2 mandatory data migrations would occur:

1. During the initial data migration; and
2. During final implementation of the system

The tenderer should also include the anticipated issue resolution timeframes in relation to data upload and migration errors.

It is expected that the tenderer covers all costs associated with creating and running reports that would ensure no loss of employee and financial data when migrating from current systems to the new system.

The Australia Council runs a payroll of up to approximately 150 people.

Responses should also detail:

- Any helpdesk support costs
- Projected Software Release schedule
- Any ongoing support costs

The tenderer will respond to the Payroll and Timesheet System IT Security Questionnaire and IT Procurement Guideline. This will be with as much detail surrounding the personal identifiable, data protection information measures and IT services management aspects of the system.

It is expected that the Australia Council will be allowed to perform annual third-party penetration testing on the tenderers system. It is also expected that the following reports would be made available to the Australia Council:

- Penetration tests
- Vulnerability reports
- ASAE 3402 reports

The tenderer agrees to comply with the Australia Council's IT Security Policy (Appendix 1). The tenderer will submit any details of why they would not be able to comply with the IT Security Policy.

B4. PERFORMANCE STANDARDS REQUIRED

The successful tenderer will be expected to achieve a high-performance standard. The Australia Council will monitor performance through a minimum of quarterly meetings with the provider.

Communications Standards

All formal reporting will adhere to the Australia Council Style Guide, which outlines the organisations accepted conventions for spelling, grammar and style.

The Australia Council is committed to communicating in ‘plain English’. The successful tenderer must ensure that all reports are written in plain, clear English, and are precise, clear, readable and efficient.

Supplier Code of Conduct

The successful tenderer will be required to adhere to the Australia Council's Supplier Code of Conduct (Appendix 2) which will form part of the terms and conditions of their contract.

B5. SPECIFIC RISKS AND/OR ISSUES

The tenderer is expected to include its risk management strategy including risks or issues involved or identified and how these risks will be managed.

B6. TIMEFRAMES

The work is expected to commence on 13 March 2023 to allow for transition to the new system to be completed by or before the implementation date of 5 July 2023.

B7. GOVERNANCE

The contractor will report to the HR Manager.

The HR Manager reports to the Director HR and Facilities.

The Director HR and Facilities reports to the Executive Director, Corporate Resources.

B8. QUOTATION

Your quote should include a comprehensive pricing breakdown including and noting GST where applicable.

EVALUATION OF TENDERS

B9. CRITERIA

The Australia Council will appoint a Tender Evaluation Committee (TEC) to review and select the successful tender against the following criteria:

Criteria	Weighting
Demonstrated understanding, knowledge and experience of payroll and timesheet processing and the application of related Federal Government legislation	35%
Proposed methodology (or delivery plan) to achieve the outcomes required including the "go live" date of 5 July 2023	30%
Ease of use by the administrator and end user enabling an efficient and streamlined approach to utilising (end user) and implementing (administrator) the product	15%
Assessment of the IT security response and posture	15%

Value for money and cost effectiveness	5%
Non weighted essential criteria	
Confirmation of the ability to commence the work on 13 March 2023	
Acceptance of the draft Terms and Conditions of the Contract (see Part C)	
Evidence of all insurances required to perform the contract	

B10. YOUR SUBMISSION COMPLYING WITH ALL PARTS OF THIS TENDER

Please note that in this evaluation, the Australia Council may seek information and referee reports from other sources. The selection of a preferred Tenderer will be based on the most efficient outcome for the Australia Council, and this involves assessing value for money and quality of service against this RFT.

PART C - GENERAL TERMS AND CONDITIONS OF CONTRACT

1. Definitions

In this Contract:

"Australia Council" means the Australia Council for the Arts, ABN 38 392 626 187.

"Contract Price" means the total contract price specified in Part 1, including any GST component payable unless otherwise specified, but for the purposes of the Payment clause of the General Conditions of Contract only, does not include any simple interest payable on late payments.

"Contractor" means the person or company engaged to undertake the Services specified in Part 1.

"Encumbrance" means a security interest as defined in section 12 of the *Personal Property Securities Act 2009* (Cth).

"Force Majeure Event" means an event beyond the control of any of the Parties, which prevents a Party or Parties from complying with any of its obligations under this Agreement, including but not limited to:

- A natural disaster such as, but not limited to, violent storm, cyclone, typhoon, hurricane, tornado, blizzard, earthquake, volcanic activity, landslide, tidal wave, tsunami, flood, damage or destruction by lightning, drought, explosion, fire;
- Acts of war, whether declared or not, acts of threats of terrorism, acts of civil unrest or disobedience, invasion, act of foreign enemies, mobilisation, requisition, or embargo; rebellion, revolution, insurrection, or military or usurped power, or civil war;
- Plague, epidemic, pandemic, outbreaks of infectious disease or any other public health crisis, including quarantine or other restrictions; act of authority whether lawful or unlawful, compliance with any law or governmental order, rule, regulation or direction, curfew restriction;
- Other unforeseeable circumstances beyond the control of the Parties against which it would have been unreasonable for the affected party to take precautions and which the affected party cannot avoid even by using its best efforts.

"Goods and/or Services" means:

(a) the Goods, Services, or Goods and Services specified in the Statement of Work; and

(b) all such incidental Goods and Services that are reasonably required to achieve the purposes of the Australia Council as specified in the Statement of Work.

"GST" means a Commonwealth goods and services tax imposed by the *GST Act.*

"GST Act" means *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

"Intellectual Property" means all intellectual property rights which may subsist in Australia or elsewhere, whether or not they are registered or capable of being registered.

"Material" means any material brought into existence as a part of, or for the purpose of producing the Goods and/or Services, and includes but is not limited to documents, equipment, information or data stored by any means.

"Moral Rights" has the same meaning given in the *Copyright Act* 1968.

"**Partner**" or "**partnership**" refers to parties' collaborative approach to fulfilling the objectives of the Contract and not to a legal relationship which subsists between persons carrying on a business in common with a view of profit.

"Special Conditions" means the special conditions attached to this Contract required by the Australia Council (if any).

"Specified Personnel" means the personnel specified in the Contract to provide the Services.

2. Provision of Services

The Contractor must provide the Services to the Australia Council on the date agreed and in accordance with any instructions for the delivery of the Services specified in writing.

The Contractor must promptly notify the Australia Council if the Contractor becomes aware that it will be unable to provide all or part of the Services by the relevant delivery date and advise the Australia Council as to when it will be able to do so.

Any Services must be provided to the standard that would be expected of an experienced and professional contractor of similar services and any other standard specified in Part 1.

Any Services must be provided free from all Encumbrances and must meet any standard specified in this contract, unless otherwise stated or agreed.

3. Acceptance

The Australia Council may accept or reject the relevant Services within 14 days after delivery of the Services or part thereof. If the Australia Council does not notify the Contractor of acceptance or rejection within the 14 day period, the Australia Council will be taken to have accepted the Services on the expiry of the 14 day period.

The Australia Council may reject the Services where the Services do not comply with the requirements of the Contract. If the Australia Council rejects the Services the Australia Council may:

(a) require the Contractor to repair or amend the Services, within a period determined by the Australia Council, at the Contractor's cost, so that the Services meet the requirements of the Contract; or

(b) require the Contractor to provide, at the Contractor's cost, replacement Services which meet the requirements of the Contract, within a period determined by the Australia Council; or

(c) terminate the Contract in accordance with the Termination clause of the General Conditions of Contract.

Replacement, amended or modified Services are subject to acceptance under this clause.

The Contractor will refund all payments related to the rejected Services unless replacement or amended Services are accepted by the Australia Council.

4. Title and Risk

Title to the Services transfers to the Australia Council upon their acceptance by the Australia Council in accordance with the Acceptance clause of the General Conditions of Contract.

The risk of any loss or damage to the Services remains with the Contractor until their delivery to the Australia Council.

5. Invoice

The Contractor must submit a correctly rendered invoice to the Australia Council. An invoice is correctly rendered if:

(a) it is correctly addressed and calculated in accordance with the Contract;

(b) it relates only to the Services that have been accepted by the Australia Council

in accordance with the Acceptance clause of the General Conditions of Contract;

(c) it is for an amount which, together with all previously correctly rendered invoices, does not exceed the Contract Price;

(d) it includes a purchase order number (if relevant); and

(e) it is a valid tax invoice in accordance with the GST Act.

Approval and payment of an amount of an invoice is not evidence of the value of the obligations performed by the Contractor, an admission of liability or evidence the obligations under the Contract have been completed satisfactorily but is payment on account only.

The Contractor must promptly provide to the Australia Council such supporting documentation and other evidence reasonably required by the Australia Council to substantiate performance of the Contract by the Contractor.

6. Payment

The Australia Council must pay the invoiced amount to the Contractor within 30 days after receiving a correctly rendered invoice or if this 30 day period ends on a day that is not a business day, payment is due on the next business day.

The last day of this period is referred to as the “due date”.

7. Price Basis

The Contract Price is the maximum price payable for the Services and is inclusive of all GST and all taxes, duties (including any customs duty) and government charges imposed or levied in Australia or overseas.

The Australia Council is not required to pay any amount in excess of the Contract Price including, without limitation, the cost of any travel, packaging, marking, handling, freight and delivery, licences, insurance and any other applicable costs and charges.

8. Offset

If the Contractor owes any amount to the Australia Council in connection with the Contract, the Australia Council may set off that amount, or part of it, against its obligation to pay any correctly rendered invoice.

9. Quality Assurance

Upon request by the Australia Council, the Contractor must provide the Australia Council and its nominees with access to the Contractor’s premises to undertake quality audits and quality surveillance as defined in the relevant Australian Quality Standards of the Contractor’s quality system and/or the production processes related to the Services.

10. Insurance

The Contractor must obtain and maintain such insurances and on such terms and conditions as a prudent contractor, providing services similar to the Services contracted for, would procure and maintain and if requested, must provide the Australia Council with evidence the insurances remain in force.

11. Indemnity

The Contractor indemnifies the Australia Council, its officers, employees and contractors against any liability, loss, damage, cost (including the cost of any settlement and legal costs and expenses on a solicitor and own client basis), compensation or expense arising out of or in any way in connection with:

(a) a default or any unlawful, wilful or negligent act or omission on the part of the Contractor, its officers, employees, agents or subcontractors; or

(b) any action, claim, dispute, suit or proceeding brought by any third party in respect of any use, infringement or alleged infringement of that third party’s

Intellectual Property rights or Moral Rights;

in connection with the Services.

The Contractor's liability to indemnify the Australia Council under paragraph (a) is reduced to the extent that any wilful default or unlawful or negligent act or omission by the Australia Council, its officers, employees or contractors is proven to have contributed to the liability, loss, damage, cost, compensation or expense.

The Australia Council holds the benefit of this indemnity on trust for its officers, employees and contractors.

12. Approvals and Compliance

The Contractor must obtain and maintain any licences or other approvals required for the lawful provision of the Services and arrange any necessary customs entry for the Services if relevant.

The Contractor must comply with and ensure its officers, employees, agents and subcontractors comply with the laws from time to time in force in the State, Territory or other jurisdictions in which any part of the Contract is to be carried out and all Commonwealth laws and policies relevant to the Services.

13. Conflict(s) of Interest

The Contractor warrants that no conflict of interest exists, or is anticipated, relevant to the performance of its obligations under the Contract.
If a conflict of that kind arises, the Contractor must notify the Australia Council immediately. The Australia Council may decide in its absolute discretion, without limiting its other rights under the Contract, that the Contractor may continue to provide the Services under the Contract.

14. Warranties

The Contractor must obtain all relevant third party warranties in respect of the Services that the Australia Council receives in relation to the Contract.

15. Access to Contractor's Premises

The Contractor agrees to give the Australia Council, or its nominee, all assistance reasonably requested for any purpose associated with this Contract or any review of the Contractor's performance under the Contract. This will include, but is not limited to, access to premises, material and personnel associated with the Services and the Contract.

16. Criminal Code Acknowledgement

The Contractor acknowledges that the giving of false or misleading information to the Australia Council is a serious offence under Section 137.1 of the schedule to the *Criminal Code Act 1995*.

The Contractor must ensure that any subcontractor engaged in connection with the Contract acknowledges the information contained in this clause.

17. Waiver

If a party does not exercise (or delays in exercising) any of its rights, that failure or delay does not operate as a waiver of those rights.

18. Variation

No agreement or understanding varying or extending the Contract, including in particular the scope of the Services, is legally binding upon either party unless it is in writing and agreed to by both parties.

19. Security and Safety

When accessing any Australia Council place, area or facility, the Contractor must comply with any security and safety requirements notified to the Contractor by the Australia Council or of which the Contractor is, or should reasonably be, aware. The Contractor must ensure that its officers, employees, agents and subcontractors are aware of, and comply

with, such security and safety requirements.

The Contractor must ensure that any material and property (including security-related devices and clearances) provided by the Australia Council for the purposes of the Contract is protected at all times from unauthorised access, use by a third party, misuse, damage and destruction and returned as directed by the Australia Council.

20. Conduct at Agency Premises

The Contractor must, when using Australia Council provided premises or facilities, comply with all reasonable directions of the Australia Council, and act consistently with the behaviours set out in the Supplier Code of Conduct.

21. Contractor not to make representations

The Contractor must not represent itself, and must ensure that its officers, employees, agents or subcontractors do not represent themselves, as being an officer, employee, partner or agent of the Australia Council, or as otherwise able to bind or represent the Australia Council. The Contract does not create a relationship of employment, agency or partnership between the parties.

22. Privacy Requirement

The Contractor agrees to comply, and ensure that its officers, employees, agents and subcontractors comply, with the *Privacy Act 1988* (Cth) and do (or refrain from doing) anything required to ensure the Australia Council is able to comply with its obligations under that Act.

The Contractor will immediately notify the Australia Council if the Contractor becomes aware of a breach or possible breach of any of its obligations under this clause.

23. Confidential Information

The Parties agree not to disclose each other's Confidential Information without prior written consent unless required or authorised by law, the Australian National Audit Office or Parliament.

24. Record Keeping

The Contractor must maintain proper business and accounting records relating to the supply of the Services and allow the Australia Council or its authorised representative to inspect those records when requested.

The Contractor will provide any assistance and information required should the Australian National Audit Office wish to conduct an audit of the Contractor's accounts and records.

25. Freedom of Information (FOI) Act 1982 requirements

Where the Australia Council has received an FOI request for access to a document created by, or in the possession of the Contractor or its subcontractors that relates to the Contract and is required to be provided under the FOI Act, the Contractor must promptly provide the document to the Australia Council, on request, at no cost.

26. Commonwealth Records and *Archives Act 1983* Requirements

The Contractor must not transfer, or permit the transfer of, custody or the ownership of any Australia Council record (as defined in the *Archives Act 1983* (Cth)) without the prior written consent of the Australia Council.

27. Moral Rights

To the extent permitted by laws and for the benefit of the Australia Council, the Contractor consents, and must use its best endeavours to ensure that each author of Material consents in writing, to the use by the Australia Council of Material, even if the use may otherwise be an infringement of their Moral Rights.

You agree not to exercise any Moral Rights you may have against us in respect of the following uses of the Agreement Materials:

(a) failure to identify the authorship or any content in the Material (including without limitation literary, dramatic, artistic works and cinematograph films within the meaning of the Copyright Act 1968 (Cth);
(b) materially altering the style, format, colours, content or layout of the Material and dealing in any way with the altered **Material** or infringing copies (within the meaning of the *Copyright Act 1968* (Cth));
(c) reproducing, communicating, adapting, publishing or exhibiting any Material, including dealing with infringing copies, within the meaning of the Copyright Act 1968 (Cth), without attributing the authorship; and
(d) adding any additional content or information to the Material.

28. Notices

Any notice or communication under the Contract will be effective if it is in writing and delivered to the postal address or email address set out in this contract.

29. Specified Personnel

The Contractor must ensure that the Specified Personnel provide the Services and are not replaced without the prior consent of the Australia Council.

At the Australia Council's request, the Contractor, at no additional cost to the Australia Council, must promptly replace any Specified Personnel that the Australia Council reasonably considers should be replaced with personnel acceptable to the Australia Council.

30. Intellectual Property and copyright licences

The Australia Council will own all Intellectual Property Rights in the Agreement Materials you create as part of the Services. You assign all present and future Intellectual Property rights subsisting in Agreement Materials to us.

If the Materials contain third party proprietary rights or your own previous material, you grant us an irrevocable, perpetual, non-exclusive, worldwide, royalty free licence to use, reproduce, publish, adapt and communicate all Intellectual Property Rights included as part of the Agreement Materials so that we can enjoy the full benefit of the Services provided under this Agreement.

31. Service Levels

All formal reporting will adhere to the Australia Council Style Guides, which outline the organisations accepted conventions for spelling, grammar, style, graphs and tables.

The Australia Council is also committed to communicating in ‘plain English’. All reports will be written in plain, clear English, and be precise, clear, and readable. The Australia Council reserves the right to contract an editor should formal reports not meet these guidelines.

32. Assignment

The Contractor must not assign or subcontract any of its rights under the Contract without the prior written consent of the Australia Council.

33. Subcontracting

Subcontracting the whole or part of the Contractor’s obligations under the Contract will not relieve the Contractor from any of its obligations under the Contract.

The Contractor must make available to the Australia Council the details of all subcontractors engaged to provide the Services under the Contract. The Contractor acknowledges that the Australia Council is required to disclose such information.

The Contractor must ensure that any subcontract entered into by the Contractor for the purpose of fulfilling its obligations under the Contract imposes on the subcontractor the same obligations that the Contractor has under the Contract (including this requirement in relation to subcontracts).

34. Termination

The Australia Council may terminate the Contract in whole or in part if:

(a) the Contractor does not deliver any or all of the Services by the relevant delivery date, or notifies the Australia Council that it will be unable to deliver the Services by the relevant delivery date;

(b) the Australia Council rejects any or all of the Services in accordance with the Acceptance clause of the General Conditions of Contract;

(c) the Contractor breaches the Contract and the breach is not capable of remedy;

(d) the Contractor does not remedy a breach of the Contract which is capable of remedy within the period specified by the Australia Council in a notice of default issued to the Contractor; or

(e) the Contractor:

(i) is unable to pay all its debts when they become due;

(ii) if incorporated – has a liquidator, administrator or equivalent appointment under legislation other than the *Corporations Act 2001* (Cth) appointed to it; or

(iii) if an individual – becomes bankrupt or enters into an arrangement under Part IX or Part X of the *Bankruptcy Act 1966* (Cth).

35. Termination or Reduction for Convenience

In addition to any other rights it has under the Contract, the Australia Council, acting in good faith, may at any time terminate the Contract or reduce the scope or quantity of the Services by notifying the Contractor in writing.

The Australia Council can terminate this Agreement, or reduce its scope, even though you are not in default, at any time by giving you written notice on the grounds of a material reduction in our parliamentary appropriation.

If the Australia Council issues such a notice, the Contractor must stop or reduce work in accordance with the notice; comply with any directions given by the Australia Council and mitigate all loss, costs (including the costs of its compliance with any directions) and expenses in connection with the termination or reduction in scope.

Where the Contract is terminated under this clause, the Australia Council will be liable for payments to the Contractor only for Services accepted in accordance with the Acceptance Clause in the General Conditions of Contract, before the effective date of termination (to a maximum of the Contract Price less any payments already made), and any reasonable costs incurred by the Contractor that are directly attributable to the termination, if the Contractor substantiates these amounts to the satisfaction of the Australia Council.

The Contractor will be entitled to profits for the proportion of the Services accepted before the effective date of termination but will not be entitled to profit anticipated on any part of the Contract that is terminated or subject to a reduction in scope.

36. Force Majeure

No party shall be liable or responsible to the other party or parties, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement (except for any obligations to make payments to the other party hereunder), when and to the extent such

failure or delay is caused by a Force Majeure Event.

37. Survival

Clauses 2, 21, 22, 23, 24, 25 and 26 of the General Conditions of Contract survive termination or expiry of the Contract.

38. Dispute Resolution

For any dispute arising under the Contract:

(a) both parties will try to settle the dispute by direct negotiation as expeditiously as possible;

(b) if unresolved, the party claiming that there is a dispute will give the other party a notice setting out the details of the dispute;

(c) within five (5) business days, each party will nominate a senior representative of their organisation, not having prior direct involvement in the dispute;

(d) the senior representatives will try to settle the dispute by direct negotiation; and

(e) failing settlement within a further ten (10) business days, either the Australia Council or the Contractor may commence legal proceedings.

The Australia Council and the Contractor will each bear its own costs for dispute resolution.

Despite the existence of a dispute, the Contractor will (unless requested in writing by the Australia Council not to do so) continue its performance under the Contract.

The procedure for dispute resolution does not apply to action relating to termination or to legal proceedings for urgent interlocutory relief.

39. Compliance with Laws

The Contractor must ensure that it and all subcontractors comply with all relevant laws in connection with the Contract including any and all of its obligations under Australian tax laws.

40. General Data Protection Regulation (GDPR) (EU)

Where required the Contractor agrees to comply with the **General Data Protection Regulation (GDPR) (EU) 2016/679** and to use adequate safeguards with respect to the protection of privacy and the fundamental rights and freedoms of individuals whose personal data you process under this Services Agreement.

41. Modern slavery and the Supplier Code of Conduct

In performing the obligations under this Services Agreement, the Contractor will (and will ensure that each and any of its subcontractors will):

(a) comply with the Australia Council's Supplier Code of Conduct;

(b) comply with the *Modern Slavery Act 2018*; and

(c) take reasonable steps to mitigate and address modern slavery risks in the Contractor's or subcontractors supply chains or in any part of their business.

42. Applicable Law

The laws of New South Wales apply to the Contract.

43. Entire Agreement

The Contract represents the parties' entire agreement in relation to the subject matter and supersedes all tendered offers (except to the extent they are incorporated into the Contract in writing) and prior representations, communications, Agreements, statements and understandings, whether oral or in writing.

Appendix 1

IT SECURITY POLICY

Issue No:	2.0
Date Issued:	July 2018
Updated:	May 2022
Scheduled Review Date:	July 2024
Document Status:	FINAL
Supersedes	IT Security Policy 1.0
Prepared by:	Lassity Martin, Director IT
Approved by:	Executive

CONTENTS

1. PURPOSE

The IT Security Policy sets out the Australia Council for the Arts' information security direction and is the backbone of the Council's IT Security Management Framework (ISMF). The purpose of the ISMF is to proactively and actively identify, mitigate, monitor, and manage information security vulnerabilities, threats, and risks in order to protect the Australia Council and its assets, information, and data.

The ISMF sets the intent and establishes the direction and principles for the protection of the Australia Council's IT assets. This is to enable continuous improvement of Council's security capability and resilience to emerging and evolving security threats.

The Australia Council Executive Team demonstrates its commitment to IT security through the issue of this policy. The Executive Director, Corporate Resources is the owner of this policy and is responsible for the review and enforcing the controls provided within the policy. Key Security roles and responsibilities are described in Section 5.

2. SCOPE

This policy applies to all users or providers of Australia Council for the Arts IT resources – including (but not limited to) temporary, permanent, and casual employees; consultants and contractors; agency employees; third party suppliers, arts sector partners and visitors. This policy applies to all Australia Council IT assets, devices connected to the Australia Council network and Cloud-based systems containing Australia Council data.

3. POLICY STATEMENTS

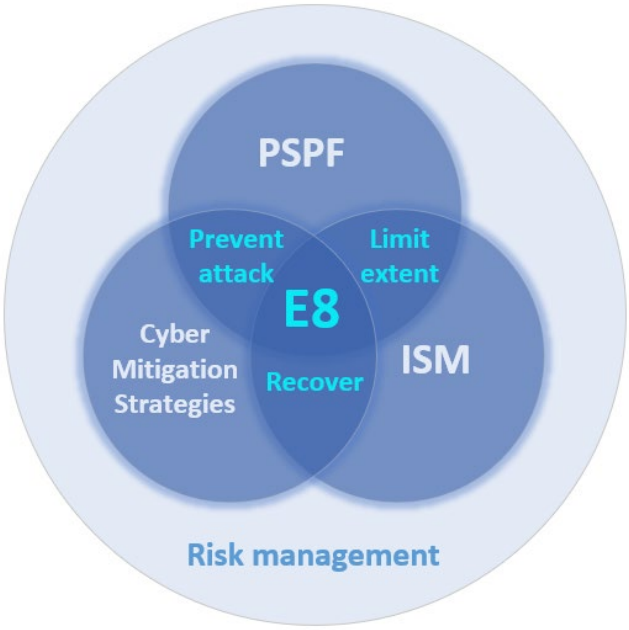
3.1 Risk-based approach to IT Security

Information security forms a part of the Australia Council's broader risk management processes. Council's approach to information security risk management is informed by the Protective Security Policy Framework (PSPF) published by the Attorney-General's Department, and the Information Security Manual (ISM) and Strategies to Mitigate Cyber Security Incidents (including the Essential Eight) produced by the Australian Cyber Security Centre (ACSC). The PSPF is not mandatory for corporate commonwealth entities such as the Australia Council, but it represents better practice guidance with respect to IT security; the ISM provides strategic and practical advice about how to protect government systems from cyber threats. The Essential Eight is a baseline set of mitigation strategies to help organisations prevent, limit the extent of and recover from cyber-attacks.

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy

- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy



ACSC "Essential Eight" alignment with other Australian government frameworks

Statement: IT suppliers and staff must take a risk-based approach to information security. Service providers and vendors must comply with Australian government protective security policies and procedures, as described in the PSPF including Policy 10: Safeguarding data from cyber threats, and adhere to any legislative or regulatory obligations under which the Australia Council operates.

Statement: The Australia Council aims to achieve a minimum of Maturity Level 2 across Essential Eight controls for Council-managed systems. The ACSC has highlighted risk associated with third party suppliers as an emerging area of concern and advised that managed service providers are a popular target for cyber-crime. Accordingly, the security posture of third-party systems hosting Council data should (at minimum) align with Essential Eight Maturity Level 3.

3.2 Application Control

Application control is a mitigation strategy to prevent execution of unapproved/malicious programs. An application whitelisting solution must be used within standard operating environments to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an approved set.

Statement: Application control must be implemented on workstations and servers to ensure that all non-approved applications (including malicious code) are prevented from executing within standard user profiles and temporary folders used by the operating system, web browsers and email clients. Allowed and blocked executions on workstations and Internet-facing servers must be logged.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to application control. Third-party systems should achieve Essential Eight Maturity Level 3.

3.3 Patch Applications

A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other program deficiencies and improving the usability or performance of the software.

Application patching is an essential control to remediate security vulnerabilities that could be used to execute malicious code on systems.

Statement: The latest versions of applications should be used wherever possible, and applications or services that are no longer supported by vendors should be removed from Council's environment. Patches, updates, or vendor mitigations for security vulnerabilities in Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software and security products must be applied within two weeks of release, or within 48 hours if an exploit exists. Other security patches should be applied within a month following their release by vendors.

A vulnerability scanner should be used on a regular basis to identify missing patches or updates for security vulnerabilities as follows:

- Daily for Internet-facing services.
- Weekly for office productivity suites, web browsers and their extensions, email clients, PDF software and security products.
- Fortnightly for other applications.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to application patching. Third-party systems should achieve Essential Eight Maturity Level 3.

3.4 Configure Microsoft Office Macro Settings

A macro is a series of commands and instructions that are grouped together as a single command to accomplish a task automatically. Microsoft Office macros are created using embedded code written in a programming language known as Visual Basic for Applications (VBA). Macros should be carefully controlled as they can be used to deliver and execute malicious code on systems.

Statement: Microsoft Office macros should be disabled for users that do not have a demonstrated business requirement. Macros in files originating from the Internet should be blocked. Antivirus scanning should be enabled for Microsoft Office macros, and they should be blocked from making Win32 API calls. Allowed and blocked Microsoft Office macro executions should be logged. Macro security settings must not be able to be changed by users.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to Microsoft Office Macro Settings. Third-party systems should achieve Essential Eight Maturity Level 3.

3.5 User Application Hardening

Application hardening is an overall term for improving the security of a given application by removing functionality that is not required and ensuring that security functionality is set at an appropriate level rather than the default settings. An example of hardening is changing the default login on a home Internet router from ‘admin’ to something unique. This is particularly important for office productivity suites such as Microsoft Office, web browsers and Internet-facing systems that are likely to be targeted by an adversary: for Example, web advertisements and Java are popular ways to deliver and execute malicious code.

To assist in securely configuring their products, vendors may provide security guides: Microsoft provides Microsoft Office security guides as part of the Microsoft Security Compliance Manager tool.

Statement: Web browsers should not process Java or web advertisements from the Internet. Internet Explorer 11 should not process content from the Internet. Microsoft Office should be configured to prevent activation of OLE packages and blocked from creating child processes, creating executable content, and injecting code into other processes. PDF software must be blocked from creating child processes. ACSC or vendor hardening guidance for Microsoft Office and PDF software must be implemented.

Web browser, Microsoft Office and PDF security settings must not be able to be changed by users. Any security functionality in applications should be enabled and configured for maximum security. Any unrequired functionality in applications should be disabled. Vendor guidance should be followed to assist in securely configuring their products.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to user application hardening. Third-party systems should achieve Essential Eight Maturity Level 3.

3.6 Restrict Administrative Privileges

Administrator accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems.

Statement: Administrative privileges to operating systems and applications should be restricted based on user duties. The need for privileges should be regularly revalidated. Privileged accounts should not be used for reading email and web browsing.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to restriction of administrative privileges. Third-party systems should achieve Essential Eight Maturity Level 3.

3.7 Patch Operating Systems

Security vulnerabilities in operating systems can be used to further the compromise of systems. Timely patching of operating systems is an essential strategy for limiting the extent of cyber security incidents.

Statement: The latest versions of operating systems should be used wherever possible. Unsupported versions should not be used. A patch management strategy must be defined covering the patching of security vulnerabilities in operating systems,

applications, drivers, and hardware devices. Systems with ‘extreme risk’ vulnerabilities should be patched within 48 hours.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to patching of operating systems. Third-party systems should achieve Essential Eight Maturity Level 3.

3.8 Multi-factor Authentication

Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Statement: Legacy authentication must not be used. Multi-factor authentication must be used to control access to Australia Council systems and data, including for VPNs, RDP, SSH and other remote access, and when users perform a privileged action or access important (sensitive/high availability) data repositories.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to multi-factor authentication. Third-party systems should achieve Essential Eight Maturity Level 3.

3.9 Regular Backups

Backups are primarily a preventative measure to protect against loss of data resulting from system failure (disaster or other), virus/malware attack, system, or human error.

Backups are an essential control and safeguard to ensure availability of Australia Council information being stored, processed, or transmitted via IT systems, and to ensure information can be accessed again following a cyber security incident (e.g. after a successful ransomware incident).

Statement: Data must be backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster. Important new/changed data, software and configuration settings should be backed up daily, stored disconnected and retained for at least three months. Test restoration of backups should be performed initially, annually, and when IT infrastructure changes.

Statement: Council-managed systems should achieve Essential Eight Maturity Level 2 with respect to regular backups. Third-party systems should achieve Essential Eight Maturity Level 3.

3.10 Security Incident Management

Provide preventive, corrective, and detective measures, ensuring a consistent and effective approach to the management of information security incidents, including communication of events and weaknesses, such as breach of access.

Well designed, understood tools and processes will help contain, preserve (legal / forensic purposes), and limit any damage resulting from a security incident.

Statement: Intrusion detection, prevention and response systems based on industry best practice must be in place for all systems containing Council data. Identified security

incidents must be handled appropriately in accordance with the Australia Council Security Incident Response Plan. Service providers and Council employees must report cyber security incidents to the Council's CISO as soon as possible after they occur or are discovered.

3.11 User Access Management

Unauthorised access to systems could enable a malicious or accidental security breach, potentially resulting in productivity, reputational or financial loss.

Only authorised users should be granted access to Australia Council systems. Access to systems and the information they process, store, or communicate is controlled through strong user identification, authentication, and authorisation practices.

Statement: All user access related requests (e.g. adding new users, updating access privileges, and revoking user access rights) must be logged, assessed, and approved in accordance with the Australia Council User Access Management Process.

Statement: Users must be uniquely identifiable, and use of shared non-user specific accounts should be avoided. Multi-factor authentication must be used to confirm the claimed identity of a user. Passwords must comply with standards defined in the IT Acceptable Use Policy.

Statement: All users must agree to comply with Council's IT Security Policy and IT Acceptable Use Policies before being granted access to Australia Council systems and data.

3.12 Logging and Monitoring

Security devices such as firewall, Intrusion detection / prevention, security event incident management, mail content filters and anti-virus all generate log data. The timely detection of information security incidents relies on comprehensive security log data being available from IT systems.

Statement: Key security-related events such as user privilege changes must be recorded in logs, protected against unauthorised changes, and analysed on a regular basis to identify potential unauthorised activities and facilitate appropriate follow up action.

3.13 Cloud Security

The Australia Council is increasingly utilising Cloud solutions to deliver business solutions and functionality. This Policy explains what the Council expects of "Cloud Service Providers" to ensure all Australia Council information and system controls, and service expectations are met.

Cloud services must maintain an appropriate level of security to ensure the confidentiality, integrity, and availability of Australia Council data. Cloud services must demonstrate a robust security posture including compliance with the ASD 'Essential Eight Strategies for Mitigating Cyber Security Incidents' at maturity level 3 or equivalent using alternative industry standards such as ISO 27001 or NIST.

Statement: When planning new business projects, Business System owners must carry out a risk assessment using the Council's Third-Party Risk Management framework to determine the impact if a system were to be compromised and consult with IT to determine appropriate security controls. Council's security requirements must be captured in contracts.

Statement: During the contract term of any Cloud service, Business System owners must:

- ensure that agreed security controls have been implemented correctly and are operating as intended.
- Report at least annually to the CISO on the security status of their systems.
- Ensure the CISO is immediately advised of any cyber security incidents and that these are managed in accordance with the Council's Cyber Security Incident Response Plan.

3.14 IT Asset Management and Configuration Control

Asset / Inventory management and configuration control is key to prudent security and management practices, providing context for all IT Security Policy statements.

Without an accurate inventory, processes such as vulnerability management are difficult to implement. For example, assessment of in scope devices when responding to critical vulnerabilities, may not be captured, hence devices will remain unpatched and therefore exposed to malicious exploit.

In the context of this policy, an IT asset is any Australia Council owned or managed device or service that connects to or is used by the Council in its business activities such as data link, physical device, application (including firmware), database and middleware.

Statement: An accurate inventory must be maintained that documents the configuration of all IT assets, including Cloud-based services that are used by Council in its business activities.

3.15 Change Management

The Australia Council IT Change Management process ensures stability and availability of related information technology communication systems across the organisation. It is important to maintain the security of systems when implementing changes.

Statement: Any change to production information systems must be logged and assessed for security and risk impact as documented in the IT Change Management Process. The requirements, risk and impact of each request must be evaluated, and the proposed risk mitigation solution must be documented and approved.

3.16 IT System Acquisition & Development

IT systems (applications, databases & middleware) are susceptible to attack and therefore security controls must be embedded throughout the whole acquisition and development lifecycle.

Statement: Appropriate security measures must be in place during all stages of IT system development, when new IT systems are implemented into the operational environment and be maintained until systems are retired.

3.17 End User Protection

End User devices are the primary gateway to Australia Council data and business applications. Implementation of appropriate information security controls is necessary to mitigate the risk of inappropriate access to data and IT systems such as malware, information disclosure or loss.

Consequently, End User protection is critical to ensuring a robust, reliable, and secure IT environment. Failing to maintain adequate controls can result in an information security incident, causing financial and/or reputational loss the Council.

Statement: End User desktop computers, mobile computers (such as laptops and tablets) must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of Australia Council data. Portable computing devices (e.g. portable hard drives, USB memory sticks etc.) should not be used unless they are encrypted.

3.18 Network Security

Network infrastructure and associated data links provide essential connectivity between internal and external systems. To provide mitigation against malicious activity, secure boundaries and connections need to be defined and managed in line with current security practices.

Statement: The Australia Council's network architecture must be commensurate with current and future business requirements as well as with emerging security threats. Appropriate controls must be established to ensure security of Council data in private and public networks, and the protection of IT services from unauthorised access.

3.19 IT Recovery

Service availability is critical for Australia Council IT communications, infrastructure, systems, and applications. This Policy ensures that processes are in place to ensure the Council's ability to recover from system and environmental failures, and regular testing of these processes is afforded.

Statement: An IT Recovery Plan and associated process must be in place to enable the recovery of business-critical Council services in a timely manner, to minimise the effect of IT disruptions and to maintain resilience before, during, and after a disruption.

4. DEFINITIONS

ACSC – the Australian Cyber Security Centre within ASD leads the Australian Government's efforts on national cyber security.

ASD – the Australian Signals Directorate is the Australian government agency responsible for foreign signals intelligence, support to military operations, cyber warfare, and information security.

Cloud - In the simplest terms, Cloud computing means storing and accessing data and programs over the Internet instead of from your computer's hard drive or on-premise server. The Cloud is a metaphor for the Internet.

End User – An End User is the person who is intended to use a computer system or device after it has been fully developed and configured. In an enterprise setting, the End User is the individual employee who uses the technology.

Essential Eight - The ACSC has developed prioritised mitigation strategies to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

Essential Eight Maturity Model – The Essential Eight Maturity Model provides advice on how to implement the Essential Eight to mitigate different levels of adversary tradecraft and targeting.

Internet - The Internet is a massive network. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer if they are both connected to the Internet.

ISM – Information Security Manual, published by the ACSC, provides strategic and practical guidance on how an organisation can protect their systems and data from cyber threats.

ISO/IEC 27001 – An international standard on how to manage information security, recognised as a best-practice framework.

IT – Information Technology

Malware - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Multi-Factor Authentication – is an authentication method in which a computer user is granted access to a given IT system only after successfully presenting two or more pieces of evidence (known as ‘factors’) to an authentication mechanism, as follows:

- something the user knows (e.g. a personal identification number (PIN), password or response to a challenge)
- something the user has (e.g. a physical token, smartcard, or software certificate)
- something the user is (e.g. a biometric value such as fingerprint or iris scan).

NIST Cybersecurity Framework – is a set of guidelines for mitigating organizational cybersecurity risks, published by the US National Institute of Standards and Technology (NIST). NIST is used by several governments and a wide range of businesses and organizations.

PSPF – the Protective Security Policy Framework is published by the Australian Government Attorney-General’s Department. It sets out government protective security policy and supports entities to effectively implement the policy across areas including security governance, information security, personnel security, and physical security.

Remote Access - refers to the ability to access an IT resource, such as a home computer or an office network computer, from a remote location. This allows Council officials to work offsite, such as at home or in another location, while still having access to a distant computer or network, such as the office network.

User - A user is a person who utilises a computer, network service or other IT resource.

User account – is an established technique for connecting a user and an IT service. A user account is comprised of a username, password and any information related to the user. User accounts determine whether a user can connect to a computer, network, or other IT resource.

Wi-Fi – a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

5. ROLES AND RESPONSIBILITIES

Role	Responsibility
Chief Security Officer (CSO) Executive Director, Corporate Resources	• Provides strategic oversight of protective security across the Australia Council. • Makes security-related decisions and fosters a positive security- culture. • Appoints security advisors to support them to deliver protective security and perform specialist services. • Works with the CISO to ensure alignment between cyber security and business objectives.
Chief Information Security Officer (CISO) – Director, IT	• Provides cyber security leadership and guidance including about procurement and vendor management. • Oversees the Council's cyber security program and ensures compliance with cyber security policy, standards, regulations, and legislation. • Implements cyber security measurement metrics and key performance indicators. • Oversees Council's response to cyber security incidents. • Coordinates security risk management activities between cyber security and business teams.
Business System Owner	• When planning new business projects, applies a risk management approach to determine the impact if a system were to be compromised. Consults with IT to assess the

	security posture of potential Cloud service providers and determine appropriate security controls. • Ensures that agreed security controls are captured in contracts and that compliance is regularly reported as part of contract management procedures. • Reports at least annually to the CISO on the security status of their systems. • Ensures the CISO is immediately advised of any cyber security incidents and that they are managed in accordance with the Council's Cyber Security Incident Response Plan.
IT Service Providers and suppliers	• Responsible for compliance with this Policy. • Responsible for the day-to-day performance of security functions.
Executive	• Be aware of this policy, encourage and ensure adherence.

6. INTERACTING POLICIES AND INFORMATION

This policy should be read in conjunction with the following related documents:

- IT Acceptable Use Policy
- Procurement of IT Services and Cloud Policy
- Out of the Office IT Access Policy
- BYOD Policy
- Code of Conduct
- Information Management Policy
- Privacy Policy
- IT Security Plan
- IT Change Management Process

The following external references are available for further information:

- Australian Government Information Security Manual (ISM) – ACSC
- Protective Security Policy Framework – Attorney-General's Department
- Essential Eight Maturity Model for Cyber Security - ACSC

7. CHANGE HISTORY

Date	Change description	Reason for change	Author	Issue no:
07/2018	Creation		Lassity Martin	1.0
05/2022	Updated format. Updated definitions, roles, responsibilities. Amended policy statements.	Updates to the Essential Eight by the ACSC; audit recommendations for policy improvement	Lassity Martin	2.0

ATTACHMENT A: THE ESSENTIAL EIGHT

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight Maturity Model, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on the ACSC's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

Appendix 2

SUPPLIER CODE OF CONDUCT

Issue No:	2.0
Date Issued:	October 2020
Updated:	December 2022
Scheduled Review Date:	December 2024
Document Status:	FINAL
Supersedes:	Version 1.0
Prepared by:	Rebecca Kenny, General Counsel
Approved by:	The Board on 9 December 2020

1 INTRODUCTION

The Australia Council for the Arts ('the Australia Council' or 'Council') is the Australian Government's principal arts funding, development and advisory body. We champion and invest in Australian arts and creativity. We support all facets of the creative process and are committed to ensuring all Australians can enjoy the benefits of the arts and feel part of the cultural life of this nation.

The Supplier Code of Conduct ('Supplier Code') sets out the standards of conduct required of a Supplier of goods and services to the Australia Council.

The Australia Council requires their Suppliers to practice the highest level of ethical and legal standards when engaged to provide goods and services. Specifically, we require our Suppliers to:

- Comply with all relevant laws and regulations;
- Implement diversity and inclusion practices and procedures within their business;
- Respect the protection of human rights by assessing and mitigating the risks of modern slavery to ensure the people and communities working within their operations and supply chains are not adversely affected by their business decisions;
- Ensure their employees and any subtractors also comply with this Supplier Code; and
- Act responsibly and honestly, with integrity and transparency, in dealing with the Australia Council.

Suppliers must comply and monitor compliance with this Supplier Code, notify the Australia Council of any breaches of this Supplier Code and take reasonable steps to address, remedy and prevent reoccurrence of any breach of the Supplier Code Principles (Part 6).

Breach of this Supplier Code may result in the Australia Council terminating its contractual relationship with a Supplier.

2 PURPOSE

The purpose of the Supplier Code is to communicate the Australia Council's expectations of and requirements for all Suppliers of goods and services to the Australia Council.

3 POLICY STATEMENT

The Australia Council values integrity and transparency when engaging with its Suppliers and seeks to work with other likeminded persons and entities that share the same principles and values.

We require our Suppliers to comply with all applicable laws and, in all cases, to, at a minimum, meet the standards and principles set out in this Supplier Code. Compliance with such laws, standards and principles is a material consideration for us in assessing our procurement processes and who we choose to do business with.

The Australia Council recognises the ethical and legal importance of protecting human rights and is committed to ensuring as far as possible the Council can identify and address any risks of modern slavery practices in its supply chains. We expect our Suppliers to share and adhere to this position.

4 SCOPE

The Australia Council requires that all its Suppliers comply with, and ensure their employees, contractors, consultants and Second Tier Suppliers are advised of and comply with this Supplier Code.

5 DEFINITIONS

Modern slavery for the purposes of this policy is defined under clause 6.4.

Modern Slavery Act 2018 means the Commonwealth legislation enacted by the Parliament of Australia on 29 November 2018 and which commenced on 1 January 2019.

Modern slavery practices are defined under Part 6.4.

Second Tier Suppliers are suppliers that provide goods and services to the Australia Council's Suppliers (defined below)

Suppliers are defined as any organisation or person who provides the Australia Council with goods or services, including their subcontractors, agents, related entities and consultants.

Supply chains is defined as the products and services (including labour) that contribute to the Australia Council's own products and services. This includes products and services sourced in Australia or overseas and extends beyond direct suppliers.

6 PRINCIPLES

The Australia Council expects Suppliers to act in an ethical and lawful manner by conducting themselves professionally and consistently with the following principles.

6.1 Compliance with the law

Suppliers must ensure that they and all their Second Tier Suppliers comply with:

- All relevant laws in connection with any legally binding contract they enter into with the Australia Council including its terms and conditions;
- All applicable laws relating to bribery, corruption, money laundering, fraud, tax evasion or similar activities including, where relevant, the Australian *Criminal Code Act 1995*;
- All relevant environmental protection laws, regulations and standards; and
- All relevant work, health and safety laws, industrial regulations as well as anti-discrimination laws for their employees, contractors and visitors in their workplace.

6.2 Governance

The Australia Council expects our Suppliers to:

- Have appropriate risk management and governance frameworks in place to ensure legal compliance and best practice standards are adhered to;
- Keep accurate records and ensure that information provided to the Australia Council is a true and accurate reflection of their operations, supply chain and business dealings;
- Have processes in place that encourage their employees and Second Tier Suppliers to report any non-compliance with this Supplier Code, anonymously if they prefer, and without retribution.

6.3 Diversity and Inclusion

The Australia Council values and supports diversity, equal opportunity and inclusion in its workplace and expects Suppliers to do the same.

Suppliers must not discriminate on the basis of gender, race (including colour, descent, nationality or ethnic origin), religion, religious belief or activity, marital/domestic status, family responsibility or parental status, pregnancy, breastfeeding, age, disability, personal associations, trade union or industrial activity, political opinion, lawful sexual activity, sexual preference, gender identity or intersex status. Discrimination based on any of the above will not be tolerated by the Australia Council.

The Australia Council respects and supports the legal status and importance of the culture, heritage and traditional rights of First Nations Australians, and requires its Suppliers to do the same.

6.4 Human Rights and Modern Slavery

The Australia Council is committed to adhering to the *Modern Slavery Act 2018* and the protection of human rights and expects its Supplier to do the same. This includes assessing

and mitigating the risks of modern slavery in the way it conducts its operations and manages its supply chains.

Modern slavery practices describe the worst and most serious types of exploitation as follows:

- **trafficking in persons** – the recruitment, harbouring and movement of a person for the purposes of exploitation through modern slavery. Exploitation also includes the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs;
- **slavery** – where the offender exercises powers of ownership over the victim;
- **servitude** – where the victim's personal freedom is significantly restricted, and they are not free to stop working or leave their place of work;
- **forced labour** – where the victim is either not free to stop working or not free to leave their place of work;
- **forced marriage** – where coercion, threats or deception are used to make a victim marry or where the victim does not understand or is incapable of understanding the nature and effect of the marriage ceremony;
- **debt bondage** – where the victim's services are pledged as security for a debt and the debt is manifestly excessive or the victim's services are not applied to liquidate the debt, or the length and nature of the services are not limited and defined;
- **the worst forms of child labour** – involves situations where children are exploited through slavery or similar practices, including for sexual exploitation or engaged in hazardous work which may harm their health or safety, or used to produce or traffic drugs; and
- **deceptive recruiting for labour or services** – where the victim is deceived about whether they will be exploited through a type of modern slavery.[1]

Suppliers must not engage, or be complicit in, any form of modern slavery practices. Any suspected or actual situations of modern slavery practices in the Supplier's business or supply chain must be reported to the Australia Council as soon as possible.

6.5 Second Tier Suppliers

The Australia Council expects that all Suppliers will have robust management processes in place for managing their own subcontractors so they can ensure that Second Tier Suppliers to the Australia Council operate in accordance with this Supplier Code.

6.6 Dealing with the Australia Council

In addition to complying with all terms and conditions of any contract entered into with the Australia Council, we require Suppliers to participate in contract performance reviews when requested and do all things reasonably necessary to protect the reputation, assets and information of the Australia Council in connection with the contract.

---

[1] Department of Home Affairs Commonwealth Modern Slavery Act 2018 - Guidance for Reporting Entities, Appendix 1, Table 5

We acknowledge that this Supplier Code cannot cover every situation or scenario and our Suppliers will also need to make judgments on their legal and ethical responsibilities. We encourage our Suppliers to engage with their contract manager in the first instance on any issues that may arise or any questions or feedback about this Supplier Code.

7 CHANGE HISTORY

Date	Change description	Reason for change	Author	Issue no:
October 2020	N/A (first version)	N/A (first version)	Rebecca Kenny, General Counsel	1.0
December 2022	Immaterial amendments to update terminology	Scheduled 2-year review	Rebecca Kenny, General Counsel	2.0