NSWPF, ICT Supplier Security Requirements

Contents

1 Introduction

The NSW Police Force (NSWPF) is committed to ensure that:

(a) existing and potential ICT Suppliers have adequate security controls in place to manage and protect NSWPF Data, Security Classified Information, and Security Classified Material; and

(b) the due diligence processes applying to existing and potential ICT Suppliers are fit for purpose to ensure the ongoing security of NSWPF assets.

2 Intended Audience

The audience for this document is ICT Suppliers (both existing and potential) and their Personnel.

3 Scope

This document sets out the Security obligations and requirements that ICT Suppliers must comply with in their dealings with NSWPF.

This NSWPF ICT Supplier Security Requirements document applies to any ICT Suppliers:

1. providing ICT goods or services to NSWPF; or
2. providing non-ICT goods or services to NSWPF, where NSWPF determines that the Security requirements set out in this document should apply in relation to the provision of those goods or services; or
3. that are transacting with NSWPF and may have access to NSWPF Data and/or NSWPF Systems), where NSWPF determines that this document should apply in relation to those transactions.

This document covers responsibilities of the ICT Supplier at organisational level, and responsibilities of the ICT Supplier and its Personnel when accessing NSWPF Systems or NSWPF Data.

NSWPF reserves the right to take any steps required to verify compliance with this document in relation to any existing and potential ICT Suppliers.

4 Security Governance

4.1 Information Security Policies

NSWPF requires that ICT Suppliers must:

a) maintain security in the delivery of the services in accordance with the Australian Government Information Security Manual (ISM) as specified under any relevant Agreement;

b) maintain an Information Security Policy that is reviewed at regular intervals (no less than annually) to respond to changing threats and risks and to cater for technology advances and provide evidence of such to NSWPF; and

c) Implement appropriate security tools and practices, including but not limited to:

i) robust cryptographic algorithms, encrypted protocols, multi-factor authentication mechanisms, network traffic inspection and filtering, security governance and security practices pertaining to its systems, premises, and Personnel when providing the services.

4.2 Security Management

NSWPF requires that ICT Suppliers:

a) provide a nominated Security Representative in relation to the provision of services to NSWPF. The Security Representative should:

i) attend security meetings with NSWPF as organised by NSWPF from time to time; and

ii) be the nominated single point of contact for security services managed and delivered by the ICT Supplier;

b) appoint a Chief Information Security Officer (CISO) or equivalent role providing cyber security leadership within the ICT Supplier's organisation in order to maintain pace with the cyber threats and ensuring compliance with cyber security policy, standards, regulations and legislation.

c) clearly nominate business owner(s) for risk, business impact and business investment strategy and technology system owner(s) for service, support and technology/system investment strategy

d) clearly nominate and supervise information security roles and responsibilities within its own organisation and follow an organisation structure where segregation of duties relating to information security is enforced and controlled;

e) address security requirements as part of the design of all aspects of delivery of services including their processes; and

f) adopt a "secure by design" approach and consider security requirements at all stages during the design and delivery of an ICT solution or service.

4.3 Ownership Changes Impacting Security

NSWPF requires that ICT Suppliers (to the extent permitted by law):

a) immediately notify NSWPF when they become aware of:

i) an actual or anticipated change in control (as defined in section 50AA of the Corporations Act 2001 (Cth)) of the ICT Supplier; or

ii) an investor domiciled outside of Australia (including foreign government investors) acquiring a substantial interest (equal to or greater than 20 per cent) of the ICT Supplier business;

b) immediately notify NSWPF if and when it becomes aware of any legal rights which may be held by another party over the ICT Supplier that could allow access to any NSWPF Data; and

c) agree that, as between NSWPF and the ICT Supplier, NSWPF retains ownership of all rights, title and interest (including intellectual property rights) in any NSWPF Data and ownership of any NSWPF Data created, developed or collected by the ICT Supplier will vest in NSWPF.

4.4 Conflicts of Interest

a) For the purposes of this section, a conflict of interest means any interest of the ICT Supplier or duty of the ICT Supplier to one or more other party that may reasonably be anticipated to conflict with or restrict the ICT Supplier in performing its obligations under a contract with NSWPF fairly and independently, including in relation to any security requirements in this document or in any contract between NSWPF and the ICT Supplier.

b) NSWPF requires that ICT Suppliers use best efforts to avoid conflicts of interest.

c) If any actual, potential or perceived conflict of interest would or could impact the Security of systems, data, Personnel or premises of NSWPF or the ICT Supplier, NSWPF expects that ICT Suppliers will notify and fully disclose this to NSWPF as soon as reasonably possible and cooperate with NSWPF to rectify the relevant conflict of interest.

4.5 Classification, Disposal and Handling of Data

This section applies to management of Supplier data ("ICT Supplier Data"). NSWPF requires that ICT Suppliers must:

a) Classify data in line with the PSPF;
b) identify information technology assets relevant in the lifecycle of data, document their importance and assign owners to assets;
c) develop or already have in place an appropriate set of procedures for information labelling and implementlabelling in accordance with the data classification;
d) document and follow policy and procedures related to the disposal of media in line with good industry practice. Media containing confidential information should be disposed of securely (e.g. by incineration or shredding, or erasure of data for use by specific applications). Guidance on how to dispose of media can be found in the ISM (*Guidelines for Media Management*). Disposal of sensitive items should be logged;
e) protect media containing data against unauthorised access, misuse or corruption at all times, including during transportation; and
f) review users' access rights at regular intervals

4.6 Classification, Disposal, and Handling of NSWPF Data by the ICT Supplier

This section applies to management of NSWPF Data. NSWPF

requires that ICT Suppliers:

a) handle NSWPF Data according to its classification as determined by NSWPF. NSWPF will follow the NSW Government Classification, Labelling and Handling Guidelines when classifying and handling NSWPF Data;
b) encrypt NSWPF Data in transit and at rest as directed by NSWPF and or in line with cryptography requirements set out in the ISM;
c) implement a decommissioning process for media to ensure that prior to final disposal, any storage media used to store NSWPF Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitised in accordance with the ISM and NSWPF Policies (such as the *Secure Disposal and Data Destruction Procedure*) to ensure that NSWPF Data cannot be retrieved from the applicable type of storage media, in whole or in part, by any data or information retrieval tools or similar means; and
d) ensure that NSWPF Data is not:
    i) used or reproduced by the ICT Supplier;
    ii) disclosed, sold, assigned, leased, sub-licensed or otherwise provided to other third- parties bythe ICT Supplier;
    iii) commercially exploited by or on behalf of the ICT Supplier, its Representatives or Personnel or;
    iv) combined with other data;

    other than as expressly authorised under its contract with NSWPF.

4.7 Subcontracting and supply chains related to NSWPF Contracts

a) NSWPF requires that the ICT Supplier will not subcontract to any other entity ("**Subcontractor**") in relation to goods or services provided to NSWPF without prior written approval by NSWPF.
b) Where approval is given, the ICT Supplier will be required to ensure that the Subcontractor complies with all requirements in this document and in any contracts(s) between NSWPF and the ICT Supplier, and that the ICT Supplier will be responsible for acts and omissions of that Subcontractor.
c) NSWPF requires that ICT Suppliers actively oversee and manage the delivery of any services by an approved Subcontractor.
d) NSWPF expects ICT Suppliers to conduct regular reviews of its suppliers and supply chain (including Subcontractors). This should include their country of origin and should identify, and subsequently rectify, any security risks that would affect the ICT Supplier and/or NSWPF.

4.8 Offshoring and Transfer of Data Overseas

a) NSWPF requires that the ICT Supplier does not:

i) subcontract or delegate any services, tasks, activities, functions or other responsibilities relating to any services, to any person who is located in a jurisdiction outside of Australia or otherwise perform those services, tasks, activities, functions or responsibilities from a jurisdiction outside of NSW;

ii) perform any services, tasks, activities, functions or other responsibilities relating to the services from a jurisdiction outside of Australia; or

iii) disclose or transfer any NSWPF Data to any person who is outside of Australia or store or process NSWPF Data in any country outside Australia.

other than as expressly authorised in any contracts(s) between NSWPF and the ICT Supplier.

b) If the ICT Supplier becomes aware of, or suspects, a failure of the ICT Supplier to comply with 4.8(a) above, NSWPF requires that the ICT Supplier promptly provide details to NSWPF and promptly follow reasonable directions from NSWPF in relation to the matter.

4.9 Conclusion of the contract between NSWPF and the ICT Supplier

NSWPF requires that ICT Suppliers, at the expiry or termination of a contract between NSWPF and the ICT Supplier, must:

a) in addition to any requirements set out in the contract with NSWPF, all NSWPF Data (both electronic and hard copy) and NSWPF assets specific to the services provided be returned to NSWPF;

b) where deletion is not constrained by legal requirements related to data retention, all NSWPF Data specific to that engagement is deleted and sanitised from the ICT Supplier's ICT systems accordance with the ISM. For further guidance see the Protective Security Policy Framework (PSPF) policy: Sensitive and classified information, the ISM Guidelines for Media Management, and NSWPF policies for guidance ondestruction of NSWPF Data; and

c) where deletion is constrained by legal requirements related to data retention, the ICT Supplier continues to comply with any applicable requirements set out in this document or the ICT Supplier's contract with NSWPF.

4.10 No Adverse Impact

NSWPF expects that ICT Suppliers will not engage with any act or omission which has or could reasonably be expected to have, an adverse impact on the security or integrity of NSWPF, its operations, its partners (includingother agencies or government entities), the services, NSWPF Systems or any NSWPF Data.

4.11 Security Self-Assessment

Where requested by NSWPF, the ICT Supplier must complete an ISM controls based self-assessment and provide results to NSWPF.

4.12 External Certifications and Assessments

a) If NSWPF requires the ICT Supplier to provide a certificate and or copy of an assessment such as the following:

i) IRAP assessments;

ii) ISM; or

iii) other certifications and assessments as requested by NSWPF on a case by case basis.

b) The security certifications provided should be relevant to the service provided.

5 Obligations when using NSWPF Systems or NSWPF Data

5.1 Access to NSWPF Systems or NSWPF Data

NSWPF requires that the ICT Supplier must:

a) only access NSWPF Systems or NSWPF Data for the purposes of the ICT Supplier carrying out, and onlyto the extent required to carry out, its obligations under its Contract(s) with NSWPF;

b) restrict access to NSWPF Systems or NSWPF Data to Personnel who have been approved and authorised by NSWPF to have such access, ensuring that:

   i) segregation of duties is defined;

   ii) the 'need to know' and the 'Least Privilege' principles are implemented; and

   iii) Role Based Access Control (RBAC) is implemented.

c) Before any of the ICT Suppliers Personnel carries out any work in connection with any NSWPF systems,the ICT Supplier must:

   i) be suitably qualified, experienced and competent to perform the services and/or be granted such access;

   ii) obtain from the ICT Suppliers Personnel any consent that is necessary to enable the NSWPF to conduct a Criminal Record Check, a baseline vetting check and any other relevant probity clearances as required by the NSWPF;

   iii) receive written confirmation from the NSWPF that those specific named Personnel are authorised to carry out work under or in connection with the ICT Services;

   iv) has been identified to NSWPF in writing, authorised under an existing Agreement or NSWPFhas given written consent;

   v) has been provided with appropriate training by the ICT Supplier to minimise the risk of accidental Security Incidents with respect to:

   vi) the correct handling and processing of NSWPF Data;

   vii) the correct handling of Security Classified Material; and

   viii) the access and use of NSWPF Systems, where so authorised;

   ix) maintains an active Australian Security Clearance, verified by NSWPF, commensurate with thesecurity classification of information and material they are accessing; and

   x) has successfully passes the pre-employment checking requirements in accordance with cl 9.1(below); and

   xi) where required by NSWPF, has signed a non-disclosure agreement directly with NSWPF;

d) the ICT Supplier acknowledges that there is lead time of approximately 10 Business Days for all clearances to be conducted and must ensure that it submits clearances within such a time to ensure that clearances are obtained prior the relevant Personnel being required to perform work under or in connection with any NSWPF systems;

e) If the ICT Supplier is unable to obtain the consent of the ICT Suppliers Personnel as required by section 5.1c) above, then, without limiting the ICT Suppliers obligations under this document, the ICT Supplier must ensure that the relevant ICT Supplier Personnel does not carry out any work in connection with any NSWPF systems and provides a suitable replacement Personnel as soon as reasonably possible. The ICT Supplier must promptly notify the NSWPF in writing if the ICT Supplier becomes aware of any change in the criminal record history, qualifications, job history or character of any of the ICT Suppliers Personnel or any other matter that may adversely affect the suitability of any of the ICT Suppliers Personnel to carry out work in connection with any NSWPF systems.

f) The NSWPF may from time to time require the ICT Supplier to withdraw any one or more of the ICT Suppliers Personnel from being engaged in connection with any of the ICT Services provided, by written notice to the ICT Supplier and without the need to provide reasons. If such written notice is issued, the ICT Supplier must immediately, to the full extent permitted by law:

i) comply with the notice;

ii) provide a replacement Personnel acceptable to the NSWPF and who meets the requirements ofthe ICT Services sought;

iii) ensure that the relevant Personnel does not carry out any work in connection to any agreementattached to the ICT Services at any time from the date of the notice, unless otherwise agreed inwriting by an authorised NSWPF representative in writing;

iv) ensure that the relevant Personnel does not have access to any information, including, withoutlimitation any NSWPF Data; and

v) ensure that any other materials of the NSWPF (if any) given to the relevant Personnel are immediately returned to the NSWPF.

g) not access NSWPF Systems or NSWPF Data from outside of Australia without prior express written consent from an authorised NSWPF representative;

h) ensure that each of its Personnel with access to NSWPF Systems is made aware of and complies with all the ICT Supplier's obligations under this Document and any contracts between NSWPF and the ICT Supplier in connection with NSWPF Systems and NSWPF Data; and

i) when accessing NSWPF Systems the ICT Supplier complies with NSWPF Code of Conduct and NSWPF Security Policies and Guidelines (e.g. *Email and Internet Guidelines*, *Secure Disposal and Data Destruction Procedure* etc.). These documents can be provided to the ICT Supplier upon request.

5.2 Remote access

a) NSWPF will only grant remote access to specific NSWPF Systems by exception, in its sole discretion, upon review of the ICT Supplier's business needs in relation to delivering the services or performing the contract with NSWPF.

b) NSWPF requires that ICT Suppliers use a NSWPF supplied remote access solution when accessing NSWPF Systems remotely. In the interests of clarity, NSWPF Remote Access in this context is any access to NSWPF where a user is not on the NSWPF wired network or NSWPF Enterprise wireless network. In such circumstances, NSWPF may provide (at its absolute discretion) a secure remote access solution which may include but not be limited to a collection of technologies (VPN, authentication, authorisation etc) for the purposes of enabling the ICT Supplier to deliver the contracted ICT Services.

6 General Information Security Requirements for ICT Supplier Systems

6.1 Data Loss Prevention

NSWPF requires that ICT Suppliers have in place appropriate software, systems and processes that are designed to detect and prevent the loss of any NSWPF Data that it holds and protect it from data leakage risks.

6.2 Protection from Malware

a) For the purposes of this section, *Harmful Code* means any computer viruses or other code that is intended or known to be harmful, destructive, disabling or which assists in or enables theft, alteration, denial of service, unauthorised disclosure or destruction or corruption of data, including viruses, worms,spyware, adware, keyloggers, trojans, ransomware and any new types of programmed threats that maybe classified as harmful code.

b) NSWPF requires that ICT Suppliers use all reasonable endeavours consistent with industry good practices including:

i) use of the most appropriate and up-to-date virus detection software and intrusion detection systems for preventing and detecting Harmful Code;

ii) implementing practices and procedures that are consistent with industry standards;

iii) pro-actively monitoring known threats of Harmful Code; and

iv) informing NSWPF of any Harmful Code and the steps necessary to avoid its introduction, to detect and prevent Harmful Code from being installed, released or otherwise introduced into (orsent from):

(1) the ICT Supplier systems used to provide the services;

(2) any deliverables to be provided to NSWPF; and

(3) any other part of NSWPF Systems.

6.3 Logging and Monitoring

a) NSWPF requires that ICT Suppliers document and implement their own Logging and Monitoring Policy describing the type of events to be generated, collected and retained.

b) NSWPF requires that the logs collected by the ICT Supplier have anti-tamper measures in place to maintain the integrity of the logs and prevent unauthorised access to those logs in order to maintain theirconfidentiality.

c) NSWPF requires that when collecting logs on behalf of NSWPF, the ICT Supplier sends all relevant logs to NSWPF logging solution and synchronises with a single reference time source provided by NSWPF.

d) NSWPF requires that when the ICT Supplier (or a Subcontractor) is hosting systems on behalf of NSWPF, logs should be retained for an agreed retention period of at least 7 years and made available to NSWPF to assist in future investigations and access control reviews.

6.4 Network security

NSWPF requires that ICT Suppliers must:

a) document and implement network security mechanisms (such as firewalls, network segregation, network traffic filtering, traffic inspection, network access control); and

b) implement encryption in transit, at the application and/or network level layer for all solutions and systems,in accordance with the standards set out in the ISM.

6.5 Security Vulnerability Management

a) NSWPF requires that ICT Suppliers document and implement a vulnerability management policy and a vulnerability management program describing how vulnerabilities will be categorised and prioritised, defining remediation timeframes, and detailing any exception mechanism.

b) NSWPF requires that ICT Suppliers ensure that all ICT Supplier systems undergo vulnerability scans:

i) on a regular basis; and

ii) immediately following any material system change,

c) Critical and Internet facing systems/services must be penetration tested prior to go-live or after significant changes/upgrades and on a regular basis as part of Systems lifecycle.

d) If a vulnerability scan or security test reveals any vulnerabilities that affect services provided to NSWPF or NSWPF Data, then NSWPF requires that the ICT Supplier report to NSWPF and remediate all material vulnerabilities, prioritised according to their severity.

6.6 Backup and Disaster Recovery

NSWPF requires that ICT Suppliers must:

a) document and implement a backup and disaster recovery process which takes regular copies of information, software and system images used in the provision of the services;

b) test their backup and disaster recovery process at least every twelve months (or as agreed in writing with NSWPF) against the ICT Supplier's backup policy with any suspected or identified defects to be remediated as soon as is reasonably possible;

c) store the backups in an encrypted format in a remote location and ensure that the encryption key(s) is/are stored securely in a separate location;

d) document and implement a disaster recovery plan;

e) test the disaster recovery plan regularly, with any suspected or identified defects to be remediated as soon as is reasonably possible; and

f) where applicable, ensure that services provided to NSWPF are backed-up according to NSWPF policy or other agreements.

6.7 Business Continuity

NSWPF requires that ICT Suppliers must:

a) document and implement a business continuity plan for use in the event of adverse situations that:

   i) identifies key business areas, critical functions, dependencies between various business areas and functions, defines acceptable downtime for each critical function and articulates a plan to maintain operations of the ICT Supplier;

   ii) is tested annually for effectiveness by the ICT Supplier; and

   iii) includes provisions to ensure the continuity of continue services delivered to NSWPF by the ICTSupplier; and

b) ensure that services and systems provided to NSWPF are available commensurate to the business or operational criticality of the services and systems to NSWPF as advised by NSWPF from time to time.

6.8 Robust Solutions and Systems

NSWPF requires that ICT Suppliers must:

a) ensure that all systems and solutions used to provide services to NSWPF are:

   i) protected from Distributed Denial of Service and Denial of Service attacks with appropriate technologies; and

   ii) monitored (performance and security), tuned, and capable of scaling to meet projections made of future capacity requirements to ensure the required system performance;

b) document operating procedures in relation to those systems and solutions, and make these procedures available to all NSWPF users who need them; and

c) establish security rules and good practices for the development of software and systems and apply them when delivering solutions and services.

6.9 System Acquisition and Development

When acquiring or developing solutions and systems critical to its business operations, NSWPF requires that ICTSuppliers must:

a) separate development, testing, and operational environments to reduce the risks of unauthorised accessor changes to the operational environment;

b) include information security related requirements in the requirements for new/existing information systems, and follow a security framework to develop or customise systems, driven by industry good practices (e.g. OWASP, CIS standards etc.);

c) implement procedures to control the installation of software on operational systems; and

d) perform security testing on sensitive/business essential solutions.

6.10 Mobile Devices, Portable Media Handling and Teleworking

ICT Suppliers must implement the following measures when accessing any NSWPF System or NSWPF

Data:

a) have a documented policy and adopt supporting security measures to manage the risks introduced by using mobile and portable devices (e.g. laptops, mobile phones);

b) seek NSWPF assessment and written approval prior to accessing NSWPF Systems or NSWPF Data from non-NSWPF provided devices;

c) have a policy and supporting security measures that are implemented to protect and avoid any information being accessed, processed or stored at Teleworking Sites;

d) not store NSWPF Data on removable media (e.g. USB stick and external hard drives); and

e) where the use of removable media is approved by NSWPF the ICT Supplier must:

   i) have in place encryption technologies using an Australian Signals Directorate (ASD) Approved Cryptographic Algorithm as per the ISM *ASD Approved Cryptographic Algorithms*; and

   ii) ensure that NSWPF Data is removed from the removable media immediately after use or at NSWPF's request in accordance with *1.6 Classification, Disposal, and Handling of NSWPF Data* by the ICT Supplier.

6.11 Controlled Access

NSWPF requires that for any ICT Suppliers System(s) that connects to NSWPF System(s) or accesses, stores, processes NSWPF Data, and any system that is used in conjunction with delivery ICT Services to NSWPF, the ICTSupplier must:

a) establish, document and review an access control policy based on business and information security requirements reflecting the premise that users should only be provided with access to the network and applications/services that they have been specifically authorised to use;

b) restrict access to data (including NSWPF Data) and application system functions in accordance with the access control policy;

c) implement an identity and access management lifecycle, including a formal user registration and de-registration process enabling assignment of access rights;

d) review and verify user access every 6 months;

e) implement a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services;

f) restrict and control privileged access rights;

g) allocate secret authentication information (e.g. passwords) through a formal management process. Authentication should be aligned with the access control policy and follow complex rules for setting passwords, and when relevant, require strong authentication (i.e. Multi-Factor Authentication (MFA));

h) implement MFA for remote access mechanisms when accessing their internet facing systems including Virtual Private Networks (VPN)s;

i) implement MFA for administrative access, and ensure that management access is segregated;

j) implement a password policy satisfying requirements for passwords as outlined in the ISM (*Guidelines forSystem Hardening*);

k) establish and maintain complete, accurate, and up-to-date records of NSWPF Data accessed, collected or changed by the ICT Supplier, which should include:

   i) details of the ICT Supplier's Personnel who accessed, collected or changed NSWPF Data;

   ii) the date it was accessed, collected or changed; and

   iii) the purpose for which it was accessed, collected or changed; and

l) ensure that only de-identified and de-personalised, sanitised data is used in non-production environments, and that NSWPF Data is not used in any non-production environment.

6.12 Email Security

NSWPF requires that ICT Suppliers must:

a) use email solutions that are securely configured (e.g. support,encryption); and

b) ensure that emails sent to and received from NSWPF:

   i) have Transport Layer Security (TLS) enforced; and

   ii) support NSWPF's enforcement of TLS for transmission of email to the ICT Supplier.

6.13 Cryptography

NSWPF requires that ICT Suppliers must:

a) establish, document, review and implement a cryptography policy based on:
   i) business and information security requirements;
   ii) the required level of protection based on the type, strength and quality of the encryption algorithm required; and
   iii) up to date cryptographic algorithms;

b) if in possession of NSWPF Data, encrypt all NSWPF Data at rest and in transit in accordance with industry good practices and where appropriate using an ASD Approved Cryptographic Algorithm as per the ISM;

c) ensure that any digital device (phone, laptop or tablet) used to access or process NSWPF Data (where so authorised under its contract(s) with NSWPF) has endpoint encryption capabilities installed using an ASD Approved Cryptographic Algorithm as per the ISM; and

d) always maintain the confidentiality of all encryption techniques such as keys secrets.

6.14 Security patching

NSWPF requires that the ICT Supplier must:

a) establish, document, review and implement a patching policy, including the need to apply security patches;

b) patch and maintain the latest vendor supported version with no unresolved vulnerabilities for its own software, operating systems and firmware. Obsolete and no longer commercially supported software,devices and equipment should be decommissioned and replaced with supported ones; and

c) patch any device, server, system, software, or network element that stores or processes NSWPF Data or connects to NSWPF Systems (where so authorised under its contract(s) with NSWPF) as soon as reasonably practicable after a security patch becomes available. New security patches should be tested in a non-production system before being released under this clause unless the patch is critical.

6.15 Use of Open Source Software

NSWPF requires that:

a) software developed on behalf of and for NSWPF should not include open source software unless agreed to in the contract between NSWPF and the ICT Supplier; and

b) before any open source software is approved, NSWPF reserves the right to conduct a security and legal review on the open source software being provided.

7 Physical Security

7.1 Secure Facilities

NSWPF requires that ICT Suppliers ensure that services are delivered from facilitates that are physically secure and environmentally maintained, with controls sufficient to prevent unauthorised physical access, damage and interference to NSWPF Data, and data storing or processing systems and facilities.

7.2 Physical Security Requirements for Security Classified Information

Where ICT Suppliers access, handle or store NSWPF Security Classified Material, NSWPF requires that ICTSuppliers must:

(a) ensure that the ICT Supplier’s premises and facilities used to access, handle or store Security Classified Material meet the PSPF’s physical security standards to protect information and assets up to, and including, the nominated security classification level; and

(b) provide NSWPF representatives access to the ICT Supplier's premises, records and equipment on request to monitor the ICT Supplier’s compliance with protective security conditions.

8 Security Incident Management

8.1 Investigations

NSWPF requires that ICT Suppliers, when requested by NSWPF, co-operate with any investigation relating to Cyber Security Incidents carried out by or on behalf of NSWPF or by any investigating body. This includes supplying any information or material in the ICT Supplier's possession or control to the extent permitted by law.

8.2 Security Incident Management

(a) ICT Suppliers must:

(i) implement technical and organisational measures to protect NSWPF Data from Security Incidents;

(ii) establish management responsibilities and procedures to ensure a quick, effective and orderly response to Security Incidents; and

(iii) retain appropriate records of the nature and circumstances of Security Incidents, any investigations, and remediation activities undertaken into the cause or possible effects of the

Security Incident for at least 7 years.

(b) At a minimum, NSWPF requires ICT Suppliers to:

(i) notify NSWPF immediately if NSWPF Systems or information are accessed or administered in anunauthorised manner or if there are reasonable grounds to suspect that unauthorised access may have taken place;

(ii) inform NSWPF of any Security Incidents including unplanned outages as soon as possible and no later than within 1 hour of becoming aware of such Security Incidents;

(iii) perform a reasonable and expeditious assessment of any Security Incidents as soon as possible and commence remediation immediately;

(iv) provide NSWPF with all details in respect of such Security Incidents;

(v) provide all reasonable assistance and support required by NSWPF so that NSWPF can assess the risk of harm arising from such Security Incidents;

(vi) investigate, mitigate and remediate such Security Incidents within the timeframes specified by NSWPF at the relevant time (depending on the critical nature of such Security Incidents);

(vii) maintain the integrity of evidence gathered during an investigation by ensuring investigators record all their actions and ensuring raw audit trails are copied onto media for archiving; and

(viii) ensure that appropriate security controls applied to protect the availability and integrity ofevidence.

9 Additional Personnel Security

9.1 Eligibility and Suitability of Personnel

In addition to the Personal Security Requirements specified under cl 2.1(c) above, ICT Suppliers must:

(a) have appropriate pre-employment checks in place as part of its onboarding process for staff and contractors. The ICT Supplier should ensure that these checks include at a minimum:

(i) confirmation of identity checks;

(ii) qualification checks;

(iii) previous employment checks; and

(iv) police checks (national criminal history);

(b) request all its Personnel to read and agree to follow the ICT Supplier's information security policy;

(c) ensure the eligibility and suitability of its Personnel who have access to NSWPF Data and NSWPFSystems (where so authorised under the ICT Supplier's contract(s) with NSWPF); and

(d) maintain a register of Personnel with access to NSWPF Data and Systems and supply this register toNSWPF upon written request.

9.2 Ongoing Training and Assessment of Personnel

ICT Suppliers must:

(a) provide appropriate security awareness education and training yearly to all Personnel, and

regular updates in organisational policies and procedures, as relevant for their job function;

(b) prevent any access to Security Classified Material by Personnel whose Australian Security Clearances are revoked, lapsed, who do not hold the appropriate security clearance, no longer have a legitimate business requirement for access or use of NSWPF Systems or access to NSWPF Data (i.e. Personnel has changed roles, duties etc) or where ICT Supplier Personnel depart the organisation;

(c) report to NSWPF in writing when any of its Personnel have had any incidental or accidental contact withSecurity Classified material;

(d) inform NSWPF in writing if any of its Personnel who are involved in providing the services to NSWPF:

(i) have been expelled from an accrediting body;

(ii) have been arrested, convicted, become a subject of criminal investigation or is undergoing disciplinary proceedings;

(iii) have or would fail any pre-employment check;

(iv) no longer require access to NSWPF Systems or NSWPF Data;

(v) have had their Australian Security Clearance revoked or have allowed it to lapse; or

(vi) have been dismissed, has resigned or are on long-term leave; and

(e) Prior to accessing NSWPF Systems or NSWPF Data ICT Supplier must ensure its authorised Personnel undertake mandatory security awareness training. ICT Supplier must further conduct regular awareness training (including the requirements pertaining to this Document) at least annually:

(i) protect NSWPF's assets and information;

(ii) report changes in personal circumstances;

(iii) report suspicious, ongoing, unusual or persistent contact; and

(iv) use ICT equipment securely and appropriately.

9.3 Change of Employment & Separating Personnel

ICT Suppliers must:

(a) require that Personnel return all the ICT Supplier organisational assets in their possession upon termination of their employment, contract or agreement;

(b) revoke the separating Personnel's physical and ICT access upon the ICT Supplier Personnel's exit fromthe ICT Supplier;

(c) immediately inform NSWPF and allow them to revoke any access provided to the separating Personnel;

(d) advise NSWPF when the Personnel with NSWPF sponsored Australian Security Clearances have ceased to work on NSWPF's contract(s);

(e) remind Personnel who have accessed NSWPF Data, Official Information, or Security Classified Information that the confidentiality requirements are ongoing. Security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the Personnel and enforced; and

(f) remove the access rights of all Personnel and external party users to data and information processing facilities upon termination of their employment, contract or agreement - or adjust access rights upon change of employment.

9.4 Disciplinary Process

NSWPF requires that ICT Suppliers have a formal and communicated disciplinary process in place to take action against Personnel who have committed or contributed to a Security breach.

Glossary of terms

Term	Definition
Australian Security Clearance	A security clearance issued by the AGSVA (Australian Government Security Vetting Agency) or an authorised vetting agency, or sponsoring entity (including NSWPF).
Australian Signals Directorate Approved Cryptographic Algorithm	A cryptographic algorithm approved by the Australian Signals Directorate and listed in the ISM (https://www.cyber.gov.au/acsc/view-all-content/guidance/asd-approved-cryptographic-algorithms).
Cyber Security Incident	A Cyber Security Incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.
Distributed Denial of Service (DDoS) and Denial of Service (DoS)	A denial-of-service attack (**DoS attack**) is a type of cyber-attack in which a threat actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. A DDoS attack is a type of DoS attack that comes from many distributed sources (e.g. botnet).
Government Agency	Means any of the following: 1. a government sector agency (within the meaning of the Government Sector Employment Act 2013 (NSW)); 2. a NSW Government agency or any other State, Territory or Federal government agency; 3. any other public authority that is constituted by or under an Act or that exercises public functions (other than a State owned corporation); or 4. any State owned corporation prescribed by regulations under the Public Works and Procurement Act 1912 (NSW).
ICT Supplier Data	ICT Supplier Data for the purposes of this Document includes data from any source and in any form, which is collected, received, stored or developed by the ICT Supplier, its employees or contractors. The data may exist in a range of forms, including: 1. documents, papers and other printed or written material; 2. electronic data; 3. voice communications; 4. video and audio recordings; 5. any physical item from which information belonging to the ICT Supplier could be derived; 6. intellectual knowledge.
NSWPF Data	NSWPF Data is any data, metadata and credentials or information in any form which is: 1. provided or made available by NSWPF or its Personnel to the ICT Supplier (including information provided for the purpose of authenticating users); 2. stored, created, generated, captured, collected, controlled, managed, processed, transferred or transmitted by NSWPF or its Personnel, or by the ICT Supplier or its Personnel on NSWPF's behalf, in the course of performing the contract or using the Services; or 3. is generated in the course of operating the ICT Supplier's business and systems in relation to the services provided to NSWPF.
NSWPF Systems	NSWPF ICT (Information and Communications Technology) Systems managed

Term	Definition
	and/or operated by or on behalf of NSWPF.
Official Information	Information that is classified as OFFICIAL or OFFICIAL: SENSITIVE under the PSPF.
Personnel	The ICT Supplier's sub-contractors, contractors, directors, officers, employees and agents, affiliates and any other person under the ICT Supplier's direction or control.
Security Classified Information	Information that is classified as PROTECTED, SECRET or TOP SECRET under the PSPF.
Security	Relating to physical security, personnel security, information security, computer security, or data security.
Security Classified Material	Media, ICT devices, systems, documents, or containers that contain Security Classified Information.
Security Incidents	A security incident can be any actual, apparent, suspected or anticipated: a. action, whether deliberate, reckless, negligent or accidental that fails to meet protective security requirements or NSWPF-specific protective security practices and procedures that results, or may result in, the loss, damage, corruption or disclosure of NSWPF Data or resources; b. a breach of a system's security policy in order to affect its confidentiality, integrity or availability and/or the unauthorised access or attempted access to a system or systems; c. approach from anybody seeking unauthorised access to NSWPF Data; d. observable occurrence or event (including natural disaster events, terrorist attacks etc) that can harm NSWPF people, NSWPF Data or NSWPF assets; or e. events which are similar to those identified in items (a) to (h) which trigger legal reporting obligations to a Federal or State governmental authority in relation to NSWPF Data. Examples include: a. Criminal actions such as actual or attempted theft, break and enter, vandalism or assault. b. Loss of personal information that is likely to result in serious harm. c. Security classified material not properly secured or stored. d. Security classified material left in inappropriate waste bins or government assets to be sold or disposed of. e. Deliberate disregard of implementing a PSPF requirement. f. An unplanned outage. g. Access passes or identification documents lost or left unsecured. h. Incorrect handling of security or classified marked information, such as failure to provide the required protection during transfer or transmission resulting in a data spill on an electronic information network or system. i. Compromise of keys to security locks, or of combination settings. j. Sharing computer passwords. For more examples, please refer to *PSPF GOVSEC02, Requirement 3*
Sensitive Information	Information that is classified as OFFICIAL: SENSITIVE under the PSPF.

Term	Definition
Subcontractor	Has the meaning given in section 1.7(a).
Teleworking Sites	A site not controlled by NSWPF or the ICT Supplier that is used for remote work by Personnel of the ICT Supplier, including but not limited to: 1. the private residence of ICT Supplier Personnel; 2. hotels, serviced apartments, and/or other accommodation used by ICT Supplier Personnel; and 3. public places such as cafes and airports used by ICT Supplier Personnel.
ICT Supplier	For the purposes of this Document, and ICT Supplier is any Party (includingPersonnel) who is either directly or indirectly: 1. providing ICT goods or services to NSWPF; or 2. providing non-ICT goods or services to NSWPF, where NSWPF determines that the Security requirements set out in this document shouldapply in relation to the provision of those goods or services; or 3. a Government Agency transacting with NSWPF (which may involve access to NSWPF Data and/or NSWPF Systems), where NSWPF determines that the Security requirements set out in this document shouldapply in relation to those transactions.