GUIDANCE PAGES TO BE DELETED WHEN PUBLISHED

ASDEFCON (SUPPORT)

SECTION 1: GUIDANCE FOR DSD-MNT-SA

(SYSTEM ADMINISTRATION SERVICES)

Status: Optional, required for contracts that include the administration of Information and Communications Technology (ICT) Systems.

Purpose: Refer to Description and Intended Use.

Policy: Refer to individual clauses.

Guidance: Drafters are to further develop this DSD to suit their requirements for the provision of Services for the administration of their particular ICT System(s) and associated Software Products.

An ICT System is any system whose primary function is to acquire, process, store, and disseminate information. An ICT System may be an administrative IT system or an operational capability, such as a surveillance system, a command-and-control system, a bespoke maintenance management system, a communications system, or some combination of all of these. If, from the perspective of the Contract, the ICT System is the primary set of Products Being Supported, then the ICT System should be treated as a Mission System and listed in section 1 of SOW Annex A. Alternatively, if the ICT System provides a support role for other Products Being Supported under the Contract (eg, a mission planning system or bespoke maintenance management system supporting a platform), then the ICT System is more likely to be treated as part of the Support System in SOW Annex A. The determination should be dependent upon the way in which the ICT System is to be managed – will the ICT System be the focus of the planning, Services, reporting, regulations and performance management under the Contract, or will that level of attention be given to a different set of Products that the ICT System supports?

This DSD may be used in conjunction with other DSDs. For example, help desk Services (described in DSD-OPS-HLPDSK) are often inter-related with system administration when the scope of the Contract includes both. Software support (in accordance with DSD-ENG-SW and DSD-ENG-SERV) will also inter-relate with this DSD when a Contract includes on-going Software development and the roll-out of Software changes. Maintenance Services for related hardware (in accordance with DSD-MNT-SERV) may also apply.

Where this DSD is used in conjunction with either or both of DSD-OPS-HLPDSK and DSD-ENG-SW, drafters may find it necessary to relocate clauses between DSDs, in order to better align the Services with expectations for how they will be managed and provided (eg, where it is anticipated that the help desk operators will also perform a number of systems administration tasks). Additionally, if only one or two clauses from one of the other DSDs is required, then they may be transferred to this DSD instead of including the other DSD in the draft Contract.

CASG and CIOG have different frameworks for defining ICT and Software support, principally due to the general differences in the nature and life-cycle of the Products that each agency manages. For CASG, support for Materiel Systems is organised and aligned to the Support System Constituent Capabilities (SSCCs), whereas CIOG uses an Information Technology Infrastructure Library (ITIL) service management framework. As CASG-supported ICT Systems may be linked to CIOG infrastructure, the CIOG support philosophy needs to be taken into account.

Related Clauses/Documents:

Refer to individual clauses

Optional Clauses: Refer to individual clauses

4 INTER-RELATIONSHIPS

Status: Core

Purpose: To identify the principle inter-related sections of the SOW, including other DSDs.

Policy: Nil

Guidance: Clause 4 should be updated to reflect the inter-related DSDs that are included in the draft Contract by tailoring clauses 4.2 to 4.5.

DSDs primarily related to ICT Systems (or just Software) are DSD-OPS-HLPDSK, DSD-ENG-SW, and this DSD. Depending on the scope of the Services, not all DSDs may be needed. In some cases, if only one or two clauses are required from one of these DSDs, it may be more efficient for management purposes to transfer the required clauses into another DSD and not use the source DSD. In other cases, drafters may find it more suitable to relocate clauses from one DSD to another, in order to better align the grouping of Services with expectations for how they will be managed and provided by the Contractor.

Related Clauses/ Documents:

DSD-OPS-HLPDSK for the provision of help desk Services

DSD-ENG-SW for the provision of Software support Services, including Software changes

DSD-MNT-MGT and DSD-MNT-SERV for the management and maintenance of ICT Systems hardware

Optional Clauses: None.

6.1.1 Scope of DSD

Status: Core

Purpose: To identify the Products Being Supported by systems administration Services.

Policy: Nil

Guidance: Drafters must ensure that each ICT System and/or the associated Software Products are appropriately incorporated into Annex A to the SOW. Applicable tables in Annex A allow for the listing of ICT Systems that are either Mission Systems or Support System RIs.

Related Clauses/Documents:

All other clauses in this DSD.

SOW Annex A, List of Products Being Supported

Optional Clauses: None

6.2.1 System Administration Planning

Status: Core

Purpose: To identify the governing plans and references applicable to system administration Services.

Policy: DSPF Principle 20

Guidance: The drafter must insert the applicable references into clause 6.2.1.1 where indicated. For security purposes, ICT Systems will need to be operated and supported in accordance with Approved Defence plans, and Contractor-developed System Security Plans and Standard Operating Procedures. For further information drafters should refer to DSPF Principle 20, COC clause 11.10, SOW clause 3.14, and the related guidance for those clauses, regarding the need for security plans and procedures.

Depending upon the nature of the Contract, the Maintenance Management Plan (MMP) may be an appropriate management plan, but in other cases it may not be appropriate as the governing plan for system administration Services. If not appropriate, an ICT System-specific plan, developed in accordance with a drafter-developed DID, may be required.

Drafters should amend the list of documents under clause 6.2.1.1 and review the remaining clauses for consistency with Contract requirements. In most cases these follow-on clauses can be retained without change.

Related Clauses/Documents:

COC clause 11.10, Defence Security

Draft SOW clause 3.14, Defence Security Compliance

Draft SOW clause 6.1, Maintenance Support Management Planning

DID-MNT-MMP, Maintenance Management Plan

Optional Clauses: None

6.2.2 Service Delivery Locations and Hours

Status: Optional

Purpose: To define the hours of operation and location requirements for Service delivery, when the Contract requires an actual physical presence at one or more locations.

Policy: TBD

Guidance: This clause is optional. If there is no requirement for the Services to be undertaken by the Contractor having a physical presence at particular sites and if there is no need to specify hours of Service delivery (eg, if addressed through assigned priorities or in response to events), then the heading should be retained and all clauses replaced with a single ‘Not used’.

The clause includes two initial options to either define Service delivery locations (Option A), or to state that no specific location is required (Option B) (ie, in cases where the ICT System can be administered remotely but clause 6.2.2 is required to define operating hours). When required, the subclauses under Option A should list the locations where system administration Services for the ICT System(s) and associated Software Products are known to require the physical presence of the system administrator(s). The drafter should check that this is consistent with the description of the ICT System(s) in Annex A to the SOW, or further develop this clause.

If an on-going physical presence is not required, then Option B should be chosen. In some cases, suitable access provisions may be needed if the Contractor’s systems administration staff will need to occasionally work on ICT Systems located at Commonwealth Premises.

If system administration is required for a set number of hours per day, then clause 6.2.2.3 is used to identify the ‘standard hours’ of system administration support at each location. If different locations require different ‘standard hours’ (eg, one location may require a 24/7 presence while support at another location may only be required from 08:00hrs to 17:00hrs on Working Days) then clause 6.2.2.3 may be substituted with the optional clauses below (when tailored appropriately). Defining the hours per day should be consistent with any related Rate of Effort description in the SOW and, where the systems administration Services also support a help desk, DSD-OPS-HLPDSK.

The final option, clause 6.2.2.4, should be included if a call-out capability (eg, by escalation of a service request from the help desk) is required. This would be used to resolve high-priority incidents when the ‘standard hours’ are not 24/7. If no call-out capability is required, then the optional clause should be deleted.

Related Clauses/Documents:

COC clause 11.10, Defence Security

Draft SOW clause 2.2, Rate of Effort

DSD-OPS-HLPDSK

Optional Clauses:

Note to drafters: Copy to clause 6.2.2.3 and amend as required.

The Contractor shall provide Services for the system administration of the ICT System(s), identified at clause 6.1.1.1, at the following locations for the designated times (‘standard hours’):

Note to drafters: Insert list of applicable locations and standard hours of support.

[... DRAFTER TO INSERT LOCATION ...] between […INSERT TIME…] and […INSERT TIME…] Eastern Standard Time / Eastern Summer Time, as applicable; and

[... DRAFTER TO INSERT LOCATION ...] between […INSERT TIME…] and […INSERT TIME…] Central Standard Time.

6.2.3 Access Administration

Status: Optional

Purpose: To define the Services for granting access to the ICT System(s) and associated Services for authorised users, while restricting access by non-authorised users.

Policy: TBD

Guidance: This clause is optional and may not be required if the Commonwealth is administering user access itself or through a separate contract for common ICT Services. If this role is to be performed by a Contractor help desk, then this clause may be transferred to DSD-OPS-HLPDSK. If not required (or if transferred), the heading should be retained and the clauses replaced with a single ‘Not used’.

Drafters should insert, in subclause 6.2.3.1a, a description of the users that will be permitted to access the ICT System. The description of system users in clause 6.2.1.1 of DSD-OPS-HLPDSK provides an example for an expanded list of users. If the list of users is the same as the help desk, subclause 6.2.3.1a may cross-reference clause 6.2.1.1 of DSD-OPS-HLPDSK.

For ICT Systems with many users, it is often impractical for the Commonwealth Representative to individually approve all user and group account access requests. Subclause 6.2.3.1b identifies that, in general, other persons are authorised to submit these requests – an example ’the authorising officer for each user group’ is given; however, this description may be amended where a more specific job title or designation is known (eg, ’XYZ system workgroup coordinators’ or ’XYZ system local site administrators’).

Clause 6.2.3.2 lists typical user access administration task requirements. Additional requirements specific to the ICT System(s), components, or specific Software applications (or for other related Services) may be detailed by including them in this clause where indicated. Services to consider, which the drafter may wish to convert to specific clauses, include those listed as optional clauses below.

Drafters should consider the times for actioning routine and urgent access requests and include these in clauses 6.2.3.3 and 6.2.3.4. Optional clause 6.2.3.5 should be included when account access can be requested through help desk Services, with the service request resolution times identified in DSD-OPS-HLPDSK. Accordingly, clauses 6.2.3.3 and 6.2.3.4 should be consistent with the times at clause 6.2.6 of DSD-OPS-HLDSK.

In the final subclause, any additional account access and management Services requirements, which are not covered in the preceding subclauses, can be added. If not required, then this place-holder clause should be deleted.

Related Clauses/Documents:

DSD-OPS-HLPDSK

Optional Clauses:

Note to drafters: Copy to clause 6.2.3.2 and amend as required.

1. provide users within designated groups with access to group resources and common data that is only available to members of that group;
2. provide designated users (eg, workgroup coordinators) with administrative control over user access to group resources and common data that is available to members of their workgroup;
3. monitor user access to Software applications with concurrent user licences, and confirm with the user that continued access is required if the user has not accessed that application within […INSERT NUMBER…] months;
4. issue hardware and/or Software (eg, ‘dongles’ or ‘tokens’) to individual users to enable access to the ICT System(s); and
5. recall hardware and Software (eg, ‘dongles’ or ‘tokens’) from individual users once the requirement for access has concluded.

6.2.4 System Event Monitoring

Status: Optional

Purpose: The purpose of this clause is to include requirements for the monitoring of the ICT System(s) to identify a need for action based on detectable user and system behaviour and conditions. The aim of such monitoring is to identify the need for actions to resolve problem situations that occur prior to any impact on system users, and to identify and resolve problems that are already having an impact.

Policy: TBD

Guidance: This clause is optional. It provides for monitoring of the ICT System(s) to identify conditions representing system events. Recognition of such events can assist to identify the need for systems administration actions, system Maintenance, or other action. If these tasks will not be performed by the Contractor (eg, because a separate help desk or Associated Party will), then the heading should be retained and the clauses replaced with a single ‘Not used’.

If these Services are required, clause 6.2.4.1 requires that the Contractor acknowledge the objectives of monitoring (as identified in the purpose above).

The system to be used for monitoring could be a core part of the ICT System or an external system (via an interface). Clauses 6.2.4.2 to 6.2.4.5 are optional clauses, used to identify the type of access provided to the monitoring system. Option A is for those ICT Systems where the monitoring system is either a separate system or a relatively discrete subsystem (ie, separate hardware) that interfaces with the primary ICT System in order to monitor system events and performance. If this option applies, (and Option B is deleted) drafters will need to select from sub-options (A-1) for when the Contractor has exclusive use, or (A-2) for shared access to the monitoring system (eg, the monitoring system is part of a larger system that monitors several other ICT Systems, some being supported by other contractors). Depending upon the sub-option selected, access to the monitoring system will require Government Furnished Equipment (GFE) and/or Government Furnished Services (GFS) and Attachment E must be updated accordingly.

If the monitoring system is fully embedded within the ICT System, then Option B should be chosen (and Option A deleted). In this instance it is assumed that the Contractor has access to the monitoring system as part of their access to the ICT System as a whole.

The system events to be monitored are organised into three groups; informational, warnings and exception events. Drafters should review the three sub-lists under clause 6.2.4.6, and amend the lists to suit the needs of the Contract and nature of the ICT System or Software Products. Additional requirements for monitoring may be added to these lists. Specific Services to consider, which the drafter may wish to convert to subclauses, include those listed as optional clauses below. Importantly, there should be a purpose for monitoring each type of system event listed. The measurement and recording process should also be automated, as much as possible, to avoid driving up the cost of the Contract.

System events are typically correlated to help to identify an underlying condition. The effectiveness of correlation can reduce false alarms and improve the effectiveness of corrective actions. Clause 6.2.4.7 requires the Contractor to consider the results of system event monitoring in order to help determine when further action must be taken in accordance with clause 6.2.4.8. Drafters should amend the subclause list for the criteria against which system events are checked.

Finally, clause 6.2.4.9 requires the Contractor to notify the Commonwealth if one or more system events will have a significant adverse impact and cannot be resolved within the timeframes given in clause 6.2.9 (which may refer the DSD-OPS-HLPDSK).

Related Clauses/Documents:

Attachment E, GFM and GFS

Optional Clauses:

Note to drafters: When suitable, copy desired events and parameters from the list below to clause 6.2.6 and amend as required.

1. system utilisation, measured in terms of […XYZ parameter…], logged at five minute intervals throughout the day;
2. hardware operating temperature, for components equipped with thermal sensors, logged at five minute intervals throughout the day;
3. changes to user access permissions implemented by […Commonwealth workgroup coordinators / local site administrators…];
4. processor utilisation of the ICT System servers;
5. usage, or attempted usage, of unauthorised Software or file types; and
6. the effectiveness of security features, including virus detection, virus protection events and other system security events.

6.2.5 Software Monitoring Services

Status: Optional

Purpose: To identify the availability of Software Updates from the OEM(s) and/or vendor(s).

Policy: TBD

Guidance: This clause requires the Contractor to monitor the availability of Software Updates from OEMs and/or vendors, as applicable. This may require monitoring OEM websites for Software Product updates and releases, or registering to be informed of such updates. If these tasks will not be performed by the Contractor, then the heading should be retained and the clauses replaced with a single ‘Not used’.

If this Service is required, the drafter needs to identify the Software Products for which the Contract will have these responsibilities and include these in SOW Annex A. Clause 6.2.5.1 cross-refers to the applicable Software Products in Annex A, while clause 6.2.5.2 requires the Contractor to monitor for the availability of updates. Subsequent optional clauses then deal with the incorporation of updates.

Incorporation of a Software Update may require an install script with appropriate parameters defined (eg, install location) and removal of the previous version, thereby creating a configuration change. A change may also require compatibility testing. Accordingly, a Software Change Request must be raised, whether or not the Contractor provides Software support Services, if an Associated Party develops the install scripts, or if the Software can be installed directly under clause 6.2.6.

Where the Contractor is providing Software support Services using DSD-ENG‑SW, Option B should be chosen for the Software changes to be managed under that DSD; otherwise, Option A should be chosen so that a Software Change Request is raised and provided to the Commonwealth for further action.

In those circumstances where some Software Products will be supported by the Contractor and others will not, Option C provides an alternative clause. For this option, SOW Annex A needs to clearly identify the Contractor’s responsibility regarding Software changes of various Software Products.

Options A and C both refer to a Software Change Request. Software Change Request requirements are to be included by the drafter in DID-CM-MGT-ECP, which includes both Engineering Change Proposals and Software Change Proposals.

Related Clauses/Documents:

Clause 6.2.8, Maintenance of System Records

COC clause 5, Technical Data, Software and Contract Material

Annex A to the SOW, Products Being Supported

DSD-ENG-SW, for analysis of Software Change Requests

DID-CM-MGT-ECP, which is used to define Software Change Request content

Optional Clauses: None

6.2.6 Implementation of Software Updates

Status: Optional

Purpose: To require the Contractor to implement Approved Software Updates.

Policy: Nil

Guidance: A common function of system administration Services is to implement (including the installation of) Software Updates, such as OEM updates identified through Software monitoring services (clause 6.2.5), once the applicable Software Update has been Approved. If the Contractor will not be required to implement Software Updates (ie, they are performed by another party), then the heading should be retained and the clauses replaced with a single ‘Not used’.

This clause includes two options. Firstly, where the Contractor is also responsible for developing Software changes under DSD-ENG-SW, Option A cross references to that DSD for the Software Update to be implemented as part of a Minor Change or Major Change to the Software Products.

Option B should be included when the Contractor will not be developing Software changes. For example, because these are performed by another party or because the Commonwealth will process Software Change Requests to incorporate OEM-sourced Software Updates.

Related Clauses/Documents:

Clause 6.2.8, Maintenance of System Records, for recording the implementation of Software Updates and related application kits and scripts

DSD-ENG-SW, for the management of Software Change Requests

Optional Clauses: None

6.2.7 Software Licence Management

Status: Optional

Purpose: To require the Contractor to manage Software licences and their allocation to users or hardware Products, as applicable.

Policy: TBD

Guidance: This clause is for use if the Contractor is to manage Software licences and record the allocation of Software licences to users or hardware installations. If these tasks will not be performed by the Contractor then the heading should be retained and the clauses replaced with a single ‘Not used’.

Clause 6.2.7.1 requires the Contractor to track the distribution and use of licences for which they are given responsibility to manage. This is particularly important where the number of installations or concurrent users is limited. Even in cases of corporate licences (unlimited users), such monitoring is useful to confirm that this form of licencing remains cost-effective. If not required, the clause can be deleted.

Clause 6.2.7.2 requires the Contractor to monitor any Software Products that are subject to subscription licencing (ie, Software that will only function for the period of a licence) to ensure that any required action is taken in time to avoid a gap in availability. If there are no subscription licences, the clause can be deleted.

Clause 6.2.7.3 requires the Contractor to maintain records of Software licences. The subclause list should be reviewed by the drafter and updated, where necessary, to ensure that the listed items address the Contract’s needs.

Drafters must ensure that SOW Annex A correctly annotates the Software Products for which the Contractor will have responsibility for managing licences – SOW Annex A may require further development (eg, an additional column in a table) to identify where this requirement is applied when this is not the same as the Contractor’s general Software responsibilities. The drafter should also review the standard licence management tasks and amend if required.

Related Clauses/Documents:

Clause 6.2.8, Maintenance of System Records

COC clause 5, Technical Data, Software and Contract Material

Annex A to the SOW, Products Being Supported

Optional Clauses: None

6.2.8 Maintenance of System Records

Status: Optional

Purpose: To require the Contractor to record details for Software applications, application (installation) kits and scripted installation procedures.

Policy: TBD

Guidance: This clause is divided into three groups of subclauses, namely:

1. the first group (clauses 6.2.8.1 to 6.2.8.3), which addresses Configuration Management (CM) responsibilities for the ICT System(s);
2. the second group (clauses 6.2.8.4 to 6.2.8.8), which includes options for identifying the applicable recording system; and
3. the third group (clauses 6.2.8.9 to 6.2.8.12), which are used to identify the details to be recorded for applications, application kits, scripted installation procedures, and their distribution.

If these tasks will not be performed by the Contractor, then the heading should be retained and the clauses replaced with a single ‘Not used’. If the Software Products are of a nature where either application kits or scripted installation will not be necessary, then the applicable subclauses can be deleted and clause 6.2.8.12 amended accordingly.

System records should be a component of CM records, and much of the required information, identified under clauses 6.2.8.9 to 6.2.8.12, may already be captured by the Configuration Status Accounting (CSA) system for the ICT System(s). As such, the first set of optional clauses identifies who has responsibility for managing the configuration of the ICT System(s). If the Contractor has this responsibility under the Contract, then drafters should select Option B; otherwise, select Option A for the Contractor to provide the requisite information to the responsible party (ie, Commonwealth or an Associated Party).

The second group of clauses addresses the record-keeping system or ‘tool’, and are only relevant if the Contractor will not have CM responsibilities for the ICT System(s) and will not use the CSA system defined under DSD-ENG-CM to maintain the required system records identified by clauses 6.2.8.9 to 6.2.8.12. If both of these conditions are true, then clauses 6.2.8.4 to 6.2.8.8 are not required and should be deleted. If either of the conditions are not true, then clauses 6.2.8.4 to 6.2.8.8 enable the required record-keeping system to be identified. Drafters should select either Option A, for a Commonwealth record-keeping system with sub-options for hardware provided by the Commonwealth or for shared resources, or Option B for the Contractor to use their own record-keeping system.

The third group of clauses (ie, clauses 6.2.8.9 to 6.2.8.12) list the system details to be recorded. Where the Contractor will have CM responsibilities and will use the CSA system defined under DSD-ENG-CM to maintain the required system records, drafters should ensure that any additional requirements included here do not conflict or duplicate the records required to be maintained by the Contractor as part of CM Services. Where additional detail is required, drafters should amend the draft clauses to include the required fields. The types of system records that might need to be managed (as addressed by the four clauses) include:

1. application records,
2. application kit records,
3. installation script records, and
4. distribution records for the above.

Related Clauses/Documents:

Clause 6.2.7, Software Licence Management, which includes requirements for recording the licence details for each application

DSD-ENG-CM, which defines requirements for the CSA system

Draft SOW clause 3.6, Co-ordination and Co-operation, for when information is passed to another party to perform CM

Optional Clauses: None

# 6.2.9 Failure Resolution

Status: Core

Purpose: To define the nature of system administration Services that the Contractor is required to undertake for restoring ICT System functions to users.

Policy: TBD

Guidance: Specific requirements for resolving Failures within the identified ICT System(s) should be detailed within this clause. These requirements could vary considerably from one contract to another, depending upon the scope of Services to be performed under the Contract and the activities that are allocated to other parties (eg, whether the Contract also includes help desk Services and if the ICT System is dependent upon hardware Maintenance provided by another party).

Clause 6.2.9.1 lists the types of Failure resolution activities to be provided as system administration Services, including the requirement to transfer responsibility for Failure resolution to a Software change activity while implementing a work around solution. Drafters should tailor this list for their Contract’s individual requirements. The initial requirements listed under clause 6.2.9.1 are based on Services described in the preceding clauses and clause 6.2.10, while the latter requirements in the list refer to hardware Maintenance and to Software support (eg, for resolution of Failures via Software change) addressed by other DSDs. When Services for Software Maintenance not involving Software change are included in the Contract, drafters need to ensure that there is no overlap or conflict with clause 6.2.10.

For Failures that will be resolved via hardware Maintenance, the default clause (6.2.9.1g) refers to DSD-MNT-MGT and DSD-MNT-SERV. For particular ICT Systems (eg, command-and-control systems or surveillance systems), hardware Maintenance will require the detailed management and work provisions that are defined in these DSDs, particularly when working under an ADF regulatory / assurance framework. For other ICT System(s) (eg, an administrative IT system), the DSD-MNT-MGT and DSD-MNT-SERV templates may not be appropriate. For these types of systems, based on COTS hardware and Software, the drafter will need to develop applicable clauses for inclusion within this DSD or a stand-alone DSD for ICT Systems hardware Maintenance. Services to consider, which the drafter may wish to convert to specific clauses, include:

1. determination of the cause of ICT System problems, faults, outages, and degraded performance;
2. replacement of failed hardware components and modules;
3. periodic hardware replacement programs;
4. recommending configuration, resource or work practice changes in order to enhance performance; and
5. liaison with specific OEMs, Software suppliers, and Software support organisations regarding any ICT System problems that are beyond the Contractor’s organic capabilities to resolve.

For Failures that will be resolved by a Software change, the default clause (6.2.9.1h) refers to subsequent clauses that initiate the Software change process while requiring a workaround solution to be implemented to temporarily resolve the Failure. Where Software change is included in the scope of the Services, clause 6.2.9.5 will refer to DSD-ENG-SW and both DSD-MNT-SA and DSD-ENG-SW must be tailored to ensure that the full scope of Services to resolve Software-related Failures is captured either through these DSDs or by referral to an Associated Party (ie, where the Contractor isn’t responsible for those Software changes).

Clause 6.2.9.2 identifies that the required resolution times for Failures not involving a Software change are defined in DSD-OPS-HLPDSK by the service request resolution times. The service request resolution times in DSD-OPS-HLPDSK need to be consistent with what can realistically be achieved when system administration tasks, included in this clause 6.2.9, are required to resolve Failures.

Note that service requests managed under DSD-OPS-HLPDSK may be resolved even though the Failure that triggered the service request remains outstanding pending the development of a Software change. In this instance, a workaround can allow the service request to be ‘resolved’; however, the long term solution may require a Software change implemented through DSD-ENG-SW, or by Associated Party or OEM update. This process may take several months and be scheduled in accordance with an individual Software Change Request or as part of a six-monthly or annual Software release program, as agreed by the CCB. Accordingly, under clause 6.2.9.2 the Commonwealth can agree to different Failure resolution times to those specified in DSD-OPS-HLPDSK (eg, in a related Software Change Proposal).

If the Contract does not include DSD-OPS-HLPDSK (eg, the Contractor provides system administration Services but there is a common corporate help desk not included in the Contract), then drafters may need to insert Failure classification clauses using clause 6.2.4 from DSD-OPS-HLPDSK as a guide. Alternatively, Failure resolution times may be defined through Key Performance Indicators (KPIs) for the Contract (refer Attachment P).

For Failures that will be resolved via a Software change, drafters need to choose from the options in draft clauses 6.2.9.4, 6.2.9.5 and 6.2.9.6. Where the Contractor is providing Software support Services using DSD-ENG‑SW, Option B should be chosen for Software changes to be managed under that DSD. Alternatively, Option A requires the Software Change Request to be raised and submitted to the Commonwealth, so it can then be passed to the Associated Party responsible for performing the Software change. In those circumstances where some Software Products will be supported by the Contractor and other Software Products will not be supported by the Contractor, Option C is used. For Option C, SOW Annex A must be tailored to ensure that the responsibility for Software change, for the various Software Products, is made clear.

Related Clauses/Documents:

Clause 6.2.3, Access Administration

Clause 6.2.4, System Event Monitoring

DSD-OPS-HLPDSK, DSD-ENG-SW, DSD-MNT-MGT and DSD-MNT-SERV

Annex A to the SOW, Products Being Supported

Attachment P, if Failure resolution is subject to a KPI

DID-ENG-MGT-ECP, which includes requirements for a Software Chance Request

Optional Clauses: None

# 6.2.10 Software Maintenance Not Requiring Software Change

Status: Optional

Purpose: To require the Contractor to provide system administration Services that maintain the functionality of Software but which do not involve a Software change.

Policy: Nil

Guidance: Software Maintenance activities that do not require actual change to Software applications may be required to ensure the on-going functionality and smooth operation of the ICT System – these activities may be included in the Services under clause 6.2.10. Some Failures may also be avoided or resolved through the system administration tasks required under clause 6.2.10. If the Contract does not require Software Maintenance that does not require a Software change, then the heading should be retained and the clauses replaced with a single ‘Not used’.

The clause has two main options; Option A, where all requirements are defined within the identified technical references (ie, listed against the ICT Systems and/or Software Products in listed SOW Annex A), and Option B, where additional details for Preventive, Corrective and Adaptive Maintenance can be inserted (through Options B-1, B-2 and B-3, respectively).

When Option A is chosen, the drafter must ensure that the appropriate technical references (which define the full nature and scope of the Services) are listed in SOW Annex A against the ICT System(s) and Software Products (or in Annex D where the entry in Annex A cross-references to Annex D). Applicable technical references may also need to be provided as GFI/GFD, and listed in Attachment E.

Option B is chosen if technical references in SOW Annex A do not accurately define all of the Software Maintenance Services required (ie, they define either greater or less scope than the Contractor’s responsibilities). Depending on the scope of the required Services, any or all of Options B-1 to B-3 may be included in the draft Contract. Drafters then need to list the applicable Services under each of the selected options as follows:

1. Option B-1 for Preventive Maintenance (not requiring Software change), including cleaning-up / deleting temporary files such as installation scripts that are no longer required, virus / malware scanning, etc.
2. Option B-2 for Corrective Maintenance (not requiring Software change), including installation or reinstallation of application files.
3. Option B-3 for Adaptive Maintenance (not requiring Software change), including the update of user and system configuration files.

Related Clauses/ Documents:

Clause 6.2.9, Failure Resolution

DSD-ENG-SW for Software Maintenance requiring Software change

Optional Clauses: None

# 6.2.11 Security Accreditation Maintenance

Status: Optional

Purpose: To identify the requirement for the Contractor to obtain and maintain security accreditation for the ICT System(s), including for Software Updates.

Policy: DSPF, in particular Principle 16, Principle 20 and Principle 13.

Guidance: This clause requires the Contractor to obtain and maintain the necessary security accreditation for the ICT System(s), including any Software Updates and Software changes that are applicable to the Software Products and/or host ICT System. Most ICT Systems will require security accreditation; however, if this is not required under the Contract (eg, security accreditation for the ICT System will be managed by the Commonwealth or another contractor), then the heading should be retained and the clauses may be replaced with a single ‘Not used’.

Drafters need to identify the relevant security authority(ies) in clause 6.2.11.1, such as CIOG if the Software is hosted on infrastructure systems such as the Defence Restricted Network or Defence Secret Network. In other instances (eg, for classified Mission Systems such as ships, aircraft and command-and-control systems), a different agency (eg, Australian Signals Directorate) will be applicable. Drafters are to add the details of the relevant security authority to the clauses, where indicated. Required system / Software accreditation details, issued by the security authority(ies), are to be inserted at clause 6.2.11.2b.

If application kits / install scripts are not relevant to the Products Being Supported or do not need to be accredited, then optional clauses

6.2.11.3 and 6.2.11.4 can be deleted and clause 6.2.11.5 amended accordingly.

Related Clauses/ Documents:

COC clause 11.10, Defence Security

Draft SOW clause 3.14, for Defence Security Compliance

Optional Clauses: None

# 6.2.12 Software Retirement

Status: Optional

Purpose: To require the Contractor to manage the retirement of Software Products and the transition of support arrangements between the old and any replacement Software Product.

Policy: TBA

Guidance: The retirement of Software can have support ramifications beyond that of the Software itself and therefore additional planning and consideration is required. This clause addresses the need for the Contractor to perform this additional planning and to keep users and other affected parties informed. If this clause is not required under the Contract, the heading should be retained and the clauses replaced with a single ‘Not used’.

This clause should be used for the routine retirement of Software from the ICT System(s), such as the Software being replaced by new versions while the general functionality of the ICT System(s) is not affected. If the retirement of the Software effectively represents the end of the life of the ICT System(s) and, therefore, the end of the Contract, these requirements should be addressed through the Phase Out provisions in other parts of the template (refer COC clause 14.2 and SOW clause 2.8).

If included in the draft Contract, Drafters should review clause 6.2.12. In general, this clause may be included without alteration.

Related Clauses/ Documents:

Clause 6.2.6, Implementation of Software Updates, for the installation of new Software Products, including those that will result in the retirement of existing Software Products

DSD-ENG-SW for the development of Software changes

Optional Clauses: None

Detailed Service Description

1. DSD NUMBER: DSD-MNT-SA-V5.0
2. TITLE: SYSTEM ADMINISTRATION SERVICES
3. DESCRIPTION and intended use

This DSD describes the requirements for the provision of Services for the administration of ICT System(s) and associated Software Products, including:

system administration planning;

Service delivery locations and hours of operation;

administering access;

monitoring system events;

monitoring Software vendors for updates;

managing Software licences;

maintaining system records;

resolving Failures;

performing Software Maintenance that does not involve a Software change;

maintaining security accreditation; and

performing Software retirement.

1. INTER-RELATIONSHIPS

This DSD forms part of the SOW.

Note to drafters: Amend the following clause to suit the scope of the Services.

This DSD shall be undertaken in conjunction with DSD-OPS-HLPDSK, for direct help desk support to system operators and support staff.

This DSD shall be undertaken in conjunction with DSD-ENG-SW to effect Software changes, including corrections, enhancements and adaptations.

This DSD shall be undertaken in conjunction with DSD-ENG-CM for the Configuration Management of the ICT System(s) and associated Software Products.

This DSD shall be undertaken in conjunction with DSD-MNT-MGT and DSD-MNT-SERV for the management and conduct of related hardware Maintenance.

1. Applicable Documents

Note to drafters: Edit the list of documents in the table below to suit the requirements of this DSD. Do not include reference to Defence policy (eg, DI(G) LOG) unless the obligations for contractors are explicitly set out in the referenced policy; otherwise, these types of documents can be open to interpretation within a contract.

The following documents form a part of this DSD to the extent specified herein:

|  |  |
| --- | --- |
| 1. DSPF | 1. *Defence Security Principles Framework* |

1. Service Description
   1. Introduction
      1. Scope of DSD

The Contractor shall provide system administration Services, as described in this DSD, for the administration of the ICT Systems identified at Annex A to the SOW.

* 1. Services
     1. System Administration Planning

Note to drafters: Amend the following clauses to select the appropriate governing plan for system administration of the ICT System(s). Refer to the guidance (above) and also the SOWTG regarding SOW clause 3.14 for security plans and procedures.

The Contractor shall manage and conduct system administration in accordance with the:

[…INSERT OTHER APPLICABLE DOCUMENTS (eg, the Approved System Security Plan and Standard Operating Procedures)…] required by SOW clauses 3.14.2 and 3.14.3;

DSPF Principle 20; and

Approved […INSERT 'MMP' OR 'SSMP'…].

The Contractor shall seek Approval for any temporary exemptions from conducting system administration in accordance with the documents listed under clause 6.2.1.1, before conducting any activities that involve those exemptions.

The Contractor shall maintain a schedule of known system administration Services, projecting work effort for a period of not less than one year in advance, or until the end of the Term where that period is less than one year.

The Contractor shall provide a copy of the Contractor’s system administration schedule in the format requested and within five Working Days (or other timeframe agreed between both parties) of a written request for a copy of this schedule from the Commonwealth Representative.

* + 1. Service Delivery Locations and Hours

|  |
| --- |
| Option A: For when systems administration Services are required at specific locations.  The Contractor shall provide Services for the system administration of the ICT Systems identified at clause 6.1.1.1 at the following designated locations:  Note to drafters: Insert list of designated locations. Refer to guidance if particular work hours are applicable to different locations.  [... DRAFTER TO INSERT LOCATION ...]; and  [... DRAFTER TO INSERT LOCATION ...].  Option B: For when systems administration Services are not required at any specific location.  The provision of system administrative Services does not require the Contractor to locate Personnel at any specific location. |

|  |
| --- |
| Option: For when the work hours for system administration Services are not specified by location, or locations are not specified. If work hours are specified by location then the following clause should be deleted.  As a minimum, the Contractor shall provide system administration Services between […INSERT TIME…] and […INSERT TIME…], Eastern Standard Time / Eastern Summer Time, as applicable (‘standard hours’). |

|  |
| --- |
| Option: For when system administration Services will be provided outside of ‘standard hours’, at a reduced level of service.  The Contractor shall provide system administration Services, outside of the standard hours, for responding to and resolving system events and service requests that are classified as a class 1 Failure in accordance with clause 6.2.9. |

* + 1. Access Administration

Note to drafters: Insert details of the authorised users, typically the users of the nominated systems or systems in SOW Annex A.

For the purposes of this clause 6.2.3:

an authorised user means […INSERT APPLICABLE DESCRIPTION…]; and

an authorised request may be approved by a party other than the Commonwealth Representative (eg, the authorising officer for each user group).

The Contractor shall create, administer, and delete user accounts, user group accounts, group membership and permissions, as required, to:

provide authorised users with access to the ICT System(s) and associated resources;

provide authorised users with access to individual Software applications that require individual user or group privileges (eg, data repositories);

remove user access to the ICT System(s), associated resources, and individual Software applications when access to these are no longer required; and

Note to drafters: Insert additional clauses for specific user account services required that are not covered by the above. Refer to the guidance for this clause for optional clause examples.

[…INSERT ADDITIONAL SERVICES REQUIRED…].

Note to drafters: Amend the timeframes in the following two clauses and optional clause to reflect the requirements of the draft Contract. If these timeframes are effectively covered through the KPIs for the draft Contract, then the drafter should consider whether or not the two clauses and the subsequent option should be deleted.

The Contractor shall complete all routine requests for administering user accounts and access to ICT System(s), associated resources, and individual Software applications within [... INSERT NUMBER ...] [... INSERT TIMEFRAME (hours OR Working Days)...], during business hours, of receiving an authorised request for such access.

The Contractor shall complete all urgent requests for administering user accounts and access to ICT System(s), associated resources, and individual Software applications within [... INSERT NUMBER ...] [... INSERT TIMEFRAME (minutes OR hours)...], during business hours, of receiving an authorised request for such access.

|  |
| --- |
| Option: For when the Contractor will also provide help desk Services in accordance with DSD-OPS-HLPDSK.  The Contractor acknowledges and agrees that the time allowed to complete requests for access may be less than that specified in clauses 6.2.3.3 and 6.2.3.4 in order to provide help desk Services within the service request resolution times specified in DSD-OPS-HLPDSK. |

Note to drafters: Insert clauses for additional user account services not covered by the above.

[…INSERT ADDITIONAL SERVICES REQUIRED…].

* + 1. System Event Monitoring

Note to drafters: If monitoring of the ICT System(s) will not be included in the scope of the Contract the clauses below, under clause 6.2.4, should be deleted and replaced with ‘Not used’.

The Contractor acknowledges and agrees that the objective of monitoring the ICT System(s) identified at clause 6.1.1.1 is to:

identify a need for action based on observable behaviour and conditions; and

ensure that, to the maximum practicable extent, any problem or Failure is resolved prior to any impact on the system users.

Note to drafters: Select from the following optional clauses A (including A-1 and A-2) or B, for when the Contractor will be provided access to a Defence monitoring system that is (A) discrete but interfaces with the ICT System, or (B) an integral part of the ICT System. If the Contractor will be provided access to a discrete system, select clause A-1 and update Attachment E if the system is for their exclusive use, or clause A-2 when shared with Defence staff or another contractor.

|  |
| --- |
| Option A: For when the Contractor will be provided with access to a discrete Defence monitoring system that interfaces with the ICT System, rather than being an integral part of it. The name of the system must be inserted into the applicable clauses below.  The Commonwealth shall provide the Contractor with on-line access to the Defence monitoring system […INSERT NAME OF SYSTEM / SOFTWARE…], for the purposes of meeting the requirements of this clause 6.2.4.  Option A-1: For when the Contractor will be provided with exclusive access to the discrete Defence monitoring system.  The Commonwealth shall provide the Contractor with terminals and/or interfaces and GFS to support the use of […INSERT NAME OF SYSTEM / SOFTWARE…], as detailed in Attachment E.  Option A-2: For when the Contractor will share access to a discrete Defence monitoring system.  The Commonwealth shall provide the Contractor with access to […INSERT NUMBER…] of shared […INSERT NAME OF SYSTEM…] terminals at […INSERT LOCATION/TIME DETAILS…].  Option B: For when the Contractor will use a monitoring system that is an integral part of the ICT System.  The Contractor shall utilise the monitoring system that is an integral part of the ICT System to meet the requirements of this clause 6.2.4. |

The Contractor shall monitor the ICT System(s) to identify any detectable or discernible occurrence that has significance for the management of the ICT System(s) or the delivery of services by the system(s) (for the purposes of this DSD known as ‘system events’), including:

Note to drafters: The following subclause lists should be tailored to include the functions, events and parameters of the ICT System for which there is a purpose for monitoring.

informational events (ie, those system events that signify normal operation), which could include system events such as:

a user logs onto an application;

a job in the batch queue completes successfully;

a device has come online; and

a transaction has completed successfully;

warning events (ie, those system events that signify that a threshold is being approached), which could include system events such as:

memory utilisation on a server is currently at 65% and increasing; if it reaches 75%, response times will be unacceptably long and the operational service agreement will be breached;

more than [... INSERT NUMBER ...] users have logged on to the [... INSERT NAME OF SUB-SYSTEM OR APPLICATION ...] application concurrently;

the number of users has reached 95% of the concurrent-user Software licences available; and

the collision rate on a network has increased by 15% over the past hour; and

exception events (ie, those system events that signify an exception, such as a Failure, has occurred), which could include system events such as:

a server has gone offline;

a device reports an error code or goes offline unexpectedly;

a Software application generates an error code;

response time of a standard transaction across the network has slowed to more than 15 seconds; and

a segment of the network is not responding to routine requests.

The Contractor shall ensure that system events identified under clause 6.2.4.6 are correlated against the following criteria to enable their impact to be assessed and to ensure that the need for further action is recognised (eg, such as invoking other Services):

Note to drafters: Amend the following clause to reflect the requirements of the Contract.

impact on Mission Critical Capabilities;

impact on safety and/or the environment;

number of system users affected;

[…INSERT ADDITIONAL CRITERIA REQUIRED…]; and

other criteria defined by the Contractor.

The Contractor shall select and initiate an appropriate response to each system event based on the system event and its correlation result assessed in accordance with clause 6.2.4.7.

Note to drafters: If advice is not required, the following clause may be deleted.

The Contractor shall promptly advise the Commonwealth Representative when a system event, which indicates a Failure, is unlikely to be resolved within the time for resolution given in clause 6.2.9, and the system event:

could adversely affect, or has adversely affected, the accomplishment of a Mission Critical Capability; or

could cause, or has caused, harm to personnel or the environment.

* + 1. Software Monitoring Services

Note to drafters: If Software monitoring Services are not applicable to the scope of work, the following clauses should be deleted and replaced with a single ’Not used’.

The Contractor shall provide monitoring Services for those Software Products where the Contractor has been identified as having these responsibilities in Annex A to the SOW.

The Contractor shall monitor each Software Product to identify when a Software Update (eg, ‘service pack’, ‘hot fix’ or other update to the version of Software Product currently in use, or planned for use, by Defence) is available from the OEM or vendor, as applicable.

Note to drafters: Options A and B below allow for the Contractor to either forward the Software Change Request to a third party for resolution or, if the Contractor is also responsible for Software support of all Software Products, to apply the Software change under the scope of DSD-ENG-SW. Option C provides the ability for the Contractor to have partial responsibility for Software support for a subset of the Software Products (as defined at SOW Annex A). Refer to the guidance for further information.

|  |
| --- |
| Option A: Include when the Contractor is to refer the change request to another party.  Where the Software monitoring Services identify that a Software Product either needs to be changed or could benefit from a change, the Contractor shall develop and deliver a Software Change Request for the affected Software Product, in accordance with CDRL Line Number ENG-810.  Option B: Include when the Contractor also has responsibility for Software support.  Where the Software monitoring Services identify that a Software Product either needs to be changed or could benefit from a change, the Contractor shall raise and process a Software Change Request in accordance with the requirements of DSD-ENG‑SW.  Option C: Include when the Contractor has Software support responsibilities for only a subset of the Software Products.  Where the Software monitoring Services identify that a Software Product either needs to be changed or could benefit from a change, the Contractor shall, for those Software Products for which the Contractor:  is identified at SOW Annex A as having Software support responsibilities, the Contractor shall raise and process a Software Change Request in accordance with the requirements of DSD-ENG‑SW; and  does not have Software support responsibilities, the Contractor shall develop and deliver to the Commonwealth Representative a Software Change Request for the affected Software Product, in accordance with CDRL Line Number ENG-810. |

* + 1. Implementation of Software Updates

Note to drafters: Select from the following optional clauses depending on whether the Contractor will develop Software changes under DSD-ENG-SW, or if the Contractor will not develop Software changes but will be required to install Software updates and new applications as a system administration Service.

|  |
| --- |
| Option A: For when the Contractor will develop Software changes.  The Contractor shall implement Software Updates as Software changes in accordance with DSD-ENG-SW.  Option B: For when the Contractor will not develop Software changes but will be required to install specific Software Updates (eg, ‘service packs’ and ‘hot fixes’).  When requested by the Commonwealth Representative, the Contractor shall develop and deliver an implementation plan to adequately control the implementation of a Software Update and its impact on the ICT System.  The Contractor shall provide the implementation plan to the Commonwealth Representative for Approval.  The Contractor shall implement the Software Update for the applicable Software Product(s) in accordance with the Approved implementation plan. |

* + 1. Software Licence Management

The Contractor shall manage the distribution of Software licences for all Software Products listed at Annex A for which the Contractor is allocated that responsibility.

For Software Products that are subject to subscription licencing (ie, Software that will only function for the period of a licence), the Contractor shall monitor these subscription licences to ensure that there is no gap in functionality due to a subscription licence expiring.

The Contractor shall maintain records for all Software licences including, for each Software application or other licensed Software Product:

the total number of licences supported under this Contract;

the total number of licences on issue to Defence users;

the total number of licences available for issue;

records of licences issued, including:

the date issued;

the quantity issued;

the system on which the licences are to be used;

the Defence user responsible for the use of the licences; and

the person authorising the issue; and

details of the scope of each licence (ie, so that it is clear to all parties exactly what support is provided with the licence, such as the availability of Software Updates).

* + 1. Maintenance of System Records

Note to drafters: Select one of the following clauses depending upon whether or not the Contractor will also have Configuration Management responsibilities for the ICT System(s) under the resultant Contract.

|  |
| --- |
| Option A: Include when the Contractor is not responsible for the Configuration Management of the ICT System(s).  The Contractor shall inform the Commonwealth Representative or an Associated Party nominated by the Commonwealth Representative of the need for changes to the Configuration Status Accounting records for the ICT System(s) identified at clause 6.1.1.1.  The Contractor shall retain copies of all Software Change Requests raised by or actioned through the system administration of the ICT System(s) identified at clause 6.1.1.1.  Option B: Include when the Contractor has responsibility for Configuration Management of the ICT System(s).  For the ICT System(s) identified at clause 6.1.1.1, the Contractor shall provide Configuration Management Services in accordance with DSD-ENG-CM, including the establishment and maintenance of application, application kit and installation script records for Software Product(s), as identified under clauses 6.2.8.9 to 6.2.8.12. |

Note to drafters: The following requirements for a record-keeping system are only relevant when a tool needs to be either used or implemented that is separate from the Configuration Status Accounting system that is used for the ICT System(s).

Select from the following optional clauses A (including A-1 and A-2) or B, based on whether or not the Contractor will be provided with on-line access to a Defence record-keeping system. If a Contractor will be provided access, select clause A-1 and update the Attachment E if the system is provided for their exclusive use, or clause A-2 for shared use (shared with Defence staff or another contractor).

Training in Commonwealth-provided information systems is addressed in clause 3.17 of the SOW.

|  |
| --- |
| Option A: For when the Contractor will be provided with on-line access to a Defence record-keeping system. The name of the system must be inserted into the applicable clauses below.  The Commonwealth shall provide the Contractor with on-line access to the Defence record-keeping system […INSERT NAME OF SYSTEM / SOFTWARE…], for the purposes of meeting the requirements of this clause 6.2.8.  Option A-1: For when the Contractor will be provided with hardware and Software for a Defence record-keeping system.  The Commonwealth shall provide the Contractor with terminals and/or interfaces and GFS to support the use of […INSERT NAME OF SYSTEM / SOFTWARE…], as detailed in Attachment E.  Option A-2: For when the Contractor will share access to a Defence record-keeping system.  The Commonwealth shall provide the Contractor with access to […INSERT NUMBER…] of shared […INSERT NAME OF SYSTEM…] terminals at […INSERT LOCATION/TIME DETAILS…].  Option B: For when the Contractor will NOT be provided on-line access to a Defence record-keeping system and the Contractor will be required to implement a system with similar functionality.  The Contractor shall implement a record-keeping system to meet the requirements of this clause 6.2.8.  The Contractor shall provide all facilities and assistance reasonably required by the Commonwealth in order for the Commonwealth to access the Contractor’s record-keeping system for the duration of the Contract. |

The Contractor shall maintain application records for each application hosted on the ICT System(s) identified at clause 6.1.1.1, consisting of:

Note to drafters: Amend the following list to suit the specific requirements of the Contract.

the date on which the application was accepted by the Commonwealth under the contract in which the application was obtained;

the record of acceptance by the Commonwealth;

the name of the application;

the version and/or release number of the application;

the organisation (vendor or Defence) from which the application was sourced;

the test and trial plan for the application; and

the test and trial report for the application.

The Contractor shall maintain application kit records, for each application, consisting of:

Note to drafters: Amend the following list to suit the specific requirements of the Contract.

the date on which the application kit was accepted by the Commonwealth under the contract from which the application kit was obtained;

the record of acceptance by the Commonwealth;

the name of the application for which the application kit was produced;

the version and/or release number of the application for which the application kit was produced;

the name of the application kit;

the test and trial plan for the application kit;

the test and trial report for the application kit;

the date on which the test was conducted;

the location at which the test was conducted;

the name(s) and contact details of the tester(s);

the task or work package identifier under which the application kit was produced;

the execution environments that the application kit supports;

a set of installation instructions; and

the target platform(s).

The Contractor shall maintain installation script records, for each scripted installation procedure, consisting of:

Note to drafters: Amend the following list to suit the specific requirements of the Contract.

the date on which the scripted installation procedure was accepted by the Commonwealth under the contract from which the scripted installation procedure was obtained;

the record of acceptance by the Commonwealth;

the name of the application for which the scripted installation procedure was produced;

the version and/or release number of the application for which the scripted installation procedure was produced;

the name of the scripted installation procedure;

the test and trial plan for the scripted installation procedure;

the test and trial report for the scripted installation procedure;

the date on which the test was conducted;

the location at which the test was conducted;

the name and contact details of the tester(s);

the task or work package identifier under which the scripted installation procedure was produced;

the execution environments that the scripted installation procedure supports; and

an installation instruction.

The Contractor shall maintain distribution records for each of the following types of Software Products for the ICT System(s) identified at clause 6.1.1.1:

applications;

application kits; and

scripted installation procedures,

where each distribution record consists of:

Note to drafters: Amend the following list to suit the specific requirements of the Contract.

the date on which the Products is issued;

the organisation (Defence unit) to which the Product is issued;

the name the recipient of the Product;

the location of the recipient of the Product;

the person (eg, system manager) authorising the issue of the Product;

the name of the Product issued;

the version number of the Product issued;

the quantity (number of licences or scripts, as applicable) issued; and

for the distribution of applications, the target platform(s).

* + 1. Failure Resolution

The Contractor shall provide the following Services to resolve Failures to the ICT System(s) identified at clause 6.1.1.1, including:

resolving Failures that arise from those system events monitored in accordance with clause 6.2.4;

Note to drafters: Amend the following list to suit the specific requirements of the Contract.

restoring lost or corrupted user data;

restoring user account configurations;

restoring system configuration and, if necessary, reinstalling applications;

re-booting ICT System hardware;

Note to drafters: The preceding subclauses may need to be amended to avoid overlap when Services for Software Maintenance not involving Software change (clause 6.2.10) are included in this DSD. If clause 6.2.10 is ‘Not used’ the following subclause should be deleted.

undertaking Software Maintenance not involving Software change, in accordance with clause 6.2.10;

Note to drafters: The use of DSD-MNT-MGT and DSD-MNT-SERV and cross-references in the following clause would be appropriate if Maintenance of the ICT System hardware warrants the detailed provisions defined in those DSDs, particularly in relation to ADF regulatory / assurance framework requirements. If, however, this level of detail is not required (eg, as is often the case for administrative IT systems), then the drafter may develop appropriate provisions for inclusion in this DSD, or a stand-alone DSD, and the following clause would need to cross-refer to those provisions.

performing hardware Maintenance in accordance with DSD-MNT-MGT and DSD-MNT-SERV, where the Contractor is allocated this responsibility at Annex A to the SOW; and

Note to drafters: In the following clause, delete the cross-references to the deleted optional clauses with respect to Software changes below (links to the deleted options will be broken).

when it is determined that a change to a Software Product is required to address a Failure and a Software change request will be raised under clause [… 6.2.9.4 / 6.2.9.5 / 6.2.9.6 …], providing a temporary work-around solution to resolve the Failure.

Note to drafters: The following clause assumes that DSD-OPS-HLPDSK has been used and the Failure classifications in that DSD have been adopted. If neither of these prerequisites are true, then the following two clauses should be deleted. If the Failure classification scheme identified in DSD-OPS-HLPDSK is required, but that DSD is not being used, then drafters should copy the required subclauses and table from clause 6.2.4 of DSD-OPS-HLPDSK into this location, and then tailor as required. The following two clauses should then be modified to refer to the applicable table.

Unless otherwise agreed by the Commonwealth Representative or otherwise specified in the Contract, the Contractor shall resolve Failures in accordance with clause 6.2.9.1, within the service request resolution times for the class of Failure as defined in DSD-OPS-HLPDSK.

The Contractor is not required to resolve a Failure in accordance with clause 6.2.9.1 when the required service request resolution time, as defined in DSD-OPS-HLPDSK, is greater than the number of Working Days remaining before the expiration of the Contract.

Note to drafters: Select one of the following options. Options A and B allow for the Contractor to either forward a Software change to a third party, for Failure resolution, or if the Contractor is responsible for Software support of all Software Products, to perform the Software change under DSD-ENG-SW. Option C provides the ability for the Contractor to have responsibility for Software support for a subset of the Software Products (as defined at SOW Annex A). Refer to the guidance for further information.

|  |
| --- |
| Option A: Include when the Contractor is to refer Software changes to another party.  Where a change to a Software Product is required to resolve a Failure, the Contractor shall develop and deliver a Software Change Request for the affected Software Product in accordance with CDRL Line Number ENG-810.  Option B: Include when the Contractor also has responsibility for Software support.  Where a change to a Software Product is required to resolve a Failure, the Contractor shall raise a Software Change Request for the affected Software Product and process the Software Change Request in accordance with the requirements of DSD-ENG-SW.  Option C: Include when the Contractor has Software support responsibilities for only a subset of the Software Products.  Where a change to a Software Product is required to resolve a Failure, the Contractor shall, for those Software Products for which the Contractor:  is identified at SOW Annex A as having Software support responsibilities, the Contractor shall raise and process a Software Change Request in accordance with the requirements of DSD-ENG‑SW; and  does not have Software support responsibilities, the Contractor shall develop and deliver a Software Change Request for the affected Software Product, in accordance with CDRL Line Number ENG-810. |

* + 1. Software Maintenance Not Requiring Software Change

Note to drafters: If the Contract is to include Software Maintenance but no other ICT System administration Services, this clause may be relocated to DSD-ENG-SW.

The Contractor shall provide Services to back up, protect, perform data integrity checks and, as necessary, restore user and system data, for each ICT System identified at clause 6.1.1.1, to ensure that the user and/or system data can be restored to a previous state specifiable in time.

Note to drafters: Select from the following optional clauses when the Contractor will be required to undertake Software Maintenance that does not involve a Software change. If there is no Software Maintenance (under the Contract) that can be performed without a Software change, this clause can be deleted and replaced with ‘Not used’.

Select Option A if this Software Maintenance is fully defined through the technical references for the ICT System(s) identified at Annex A to the SOW. Select Option B by selecting one or more of the sub-options B‑1 to B‑3 to specify requirements for Preventive Maintenance, Corrective Maintenance and Adaptive Maintenance, respectively.

When specific requirements are not fully defined in the technical references identified at Annex A to the SOW, drafters may need to incorporate additional detail here to ensure that the nature and scope of the work is properly bounded (eg, in terms of specific activities required at specific locations and/or to specific Software Products and/or using particular techniques and tools). See guidance for further information.

|  |
| --- |
| Option A: For when all Software Maintenance, which does not involve a Software change, is defined through the technical references identified at Annex A to the SOW.  The Contractor shall undertake all Maintenance, which does not involve a Software change, for the Software Products specified at clause 6.1.1.1 in accordance with the technical references identified in Annex A to the SOW for those Software Products.  Option B-1: For when specific requirements in relation to Preventive Maintenance for Software, which do not involve a Software change, need to be set out in the Contract.  The Contractor shall undertake the following Preventive Maintenance activities, which do not involve a Software change, for the Software Products specified at clause 6.1.1.1:  Note to drafters: Incorporate any specific details required into the following subclauses. Examples of Preventive Maintenance, which does not involve a Software change, includes deleting temporary files, running virus scans and de-fragmenting hard drives.  […DRAFTER TO INSERT…]; and  […DRAFTER TO INSERT…].  Option B-2: For when specific requirements in relation to Corrective Maintenance for Software, which do not involve a Software change, need to be set out in the Contract.  The Contractor shall undertake the following Corrective Maintenance activities, which do not involve a Software change, for the Software Products specified at clause 6.1.1.1:  Note to drafters: Incorporate any specific details required into the following subclauses. Examples of Corrective Maintenance, which does not involve a Software change, includes reinstalling all or some of the Software, device drivers, and rebooting a system after failure.  […DRAFTER TO INSERT…]; and  […DRAFTER TO INSERT…].  Option B-3: For when specific requirements in relation to Adaptive Maintenance for Software, which do not involve a Software change, need to be set out in the Contract.  The Contractor shall undertake the following Adaptive Maintenance activities, which do not involve a Software change, for the Software Products specified at clause 6.1.1.1:  Note to drafters: Incorporate any specific details required into the following subclauses. Examples of Adaptive Maintenance, which does not involve a Software change, includes incorporating adaptation data to alter the way a system operates. Examples of adaptation data include communication plans that change protocols and radio frequencies for an operation; geographic data to adapt a system to a new location; threat data that alters a system for different threats; and configuration data that adapts a system for different roles.  […DRAFTER TO INSERT…]; and  […DRAFTER TO INSERT…]. |

* + 1. Security Accreditation Maintenance

Note to drafters: The following clauses may be applicable when Software is hosted on a secure ICT System, is a stand-alone security-rated system, or interfaces with one. These clauses require that the appropriate clauses will be included at COC clause 11.10 and SOW clause 3.14 for Defence Security requirements and compliance activities. The following clause should be amended to include the applicable authority. Reference to the Commonwealth Representative may be removed if direct consultation between the Contractor and authority is preferred and a suitable agreement with that agency is in place.

The Contractor shall consult, coordinate and cooperate with the Commonwealth Representative, [... INSERT CIOG or other Agency ...], and Commonwealth security authority(ies), to ensure that all applicable ICT System Products listed at Annex A to the SOW have a current and appropriate security accreditation for the intended operating environment in accordance with clause 3.14 of the SOW and clause 11.10 of the COC, particularly the Security Classification and Categorisation Guide at Attachment J.

The Contractor shall maintain details of security accreditation for each applicable ICT System and Software Product, including:

the current security accreditation status of the ICT System or Product; and

Note to drafters: Amend the following clause for the appropriate security accreditation reference(s).

the [... CIOG or other Agency ...] [... INSERT NAME OF 'ACCREDITATION NUMBER/ REFERENCE' ...].

|  |
| --- |
| Option: Include the following clauses if the application kits must also be security accredited.  Note to drafters: Similar to clause 6.2.11.1, involvement of and reference to the Commonwealth Representative in the following clause may be removed for direct liaison between the Contractor and the applicable agency when a suitable agreement is in place.  The Contractor shall liaise with the Commonwealth Representative and Commonwealth security authority(ies) to ensure that all application kits have a current security accreditation.  The Contractor shall maintain details of security accreditation for each application kit, including:  the current security accreditation status; and  the [... CIOG or other Agency ...] [... INSERT NAME OF 'ACCREDITATION NUMBER/ REFERENCE' ...]. |

The Contractor shall maintain a rolling twelve month schedule of security accreditation tasks for each Software Product.

* + 1. Software Retirement

The Contractor acknowledges that either the Contractor or another party may identify the need to retire a Software Product for reasons such as the Software Product is no longer supported or is no longer required or has been replaced by another Product.

Where the Contractor identifies the need to retire a Software Product, the Contractor shall develop and deliver a Software Change Request, for the retirement of the Software Product, in accordance with CDRL Line Number ENG-810.

Where the Contractor receives a Software Change Request for the retirement of a Software Product from a party other than the Commonwealth Representative, the Contractor shall forward the Software Change Request to the Commonwealth Representative for Approval.

Once a Software Change Request for the retirement of a Software Product has been Approved by the Commonwealth Representative, the Contractor shall develop and document a retirement plan to withdraw active support for the affected Software Products.

The Contractor shall consider the affected users and address the following in the retirement plan:

cessation of full or partial support after a certain period of time;

archiving of the Software Product and its associated documentation;

responsibility for any future residual support issues;

transition to the new Software Product, if applicable; and

accessibility of archive copies of data.

The Contractor shall deliver the retirement plan to the Commonwealth Representative for Approval.

The Contractor shall retire the affected Software Product in accordance with the Approved retirement plan.

The Contractor shall provide notice to affected users of the intention to retire the Software Product and include the following in the notification:

a statement explaining why the Software Product will no longer be available;

if applicable, a description of the replacement Software Product and its date of availability; and

a description of the user support options available, if any, once access to the Software Product has been removed.

At the scheduled time of retirement, the Contractor shall archive, as applicable, all configuration documentation, logs, code, scripts, and any data used by, or associated with, the retired Software Product.