| | | | |
|---|---|---|---|
| **JSP 602 Instruction** | 1024 | **Applicability** | Applications |
| **Configuration Identity** | Version: 01.02<br>Amended: 2009-03-02<br>Reviewed: 2006-06-28 | **Epoch Applicability** | 2005 - 2009 |

# JSP 602: 1024 - Operating Systems

## Outline

Description: Operating Systems provide the execution environment and local services for both clients (including portable and hand held devices) and servers. This policy specifies the permissible client and server platform configurations. There is no single operating system that will be appropriate for all of the GII, (even if a supplier produced products for all possible platforms there is no guarantee that they would be suitable for MOD and such a level of lock-in would be undesirable). Hence, to achieve coherent delivery of information services across the GII, MOD must adopt appropriate operating systems that readily support the implementation of open information services.

Reasons for Implementation: Compliance with the approach outlined in this policy leaflet will enhance interoperability through operating systems that readily support the implementation of open information services, improve corporate compatibility through the use of standard business clients, reduce training costs, reduce lock-in to a single supplier and reduce vulnerability from attack through diversification.

Issues: POSIX is the Portable Operating System Interface, an open operating interface standard developed by the IEEE. POSIX compliance makes code portability between systems more cost effective. Linux and MS Windows 2000 both support POSIX. MS Windows XP does not natively support POSIX. However, POSIX does not have a standard for GUIs, significantly limiting its usefulness.

Guidance: This policy is outside the scope of the e-GIF and the NC3TA.

The choice of Operating System is largely dependent upon the primary function of the computer on which it resides. Consequently the policy below mandates the use of a limited number of operating systems based upon that computer’s role

## Policy

**Strategic**

**1024.01: Business Client**

**1024.01.01** Systems and/or projects providing business client devices shall adopt the following:

**1024.01.01.01** Microsoft Windows

*Dominant operating system with wide product support and an established user base.*

*Comment:* A business client is a computer predominantly used for office automation tasks. The choice of OS is down to the infrastructure provider, with DII being the principal infrastructure provider for the strategic environment.

**1024.02: Workstation Clients**

**1024.02.01** Systems and/or projects providing workstation client devices shall adopt any of the following as best befits the function of the workstation:

**1024.02.01.01** Microsoft Windows

*Dominant operating system with wide product support and an established user base. This OS may be used when required applications are available and it is considered best value for money.*

**1024.02.01.02** Linux distributions that conform to the Linux Standards Base

*Widely used operating system. This OS may be used when required applications are available and it is considered best value for money.*

**1024.02.02** The following operating systems shall only to be used if the options mandated above are not suitable for the required purpose:

**1024.02.02.01** Proprietary Unix

*Widely used to support legacy systems with a large and established user base. Unix should only be used if there is a compelling reason for not using MS Windows or Linux*

**1024.02.02.02** Bespoke/Specialist Operating System

*Bespoke/specialist operating systems that offer particular features relevant to specific MOD requirements. These OSs should only be used when such requirements fall outside the scope of the more widely adopted OSs listed.*

*Comment:* A workstation client is a computer predominantly used for specific role based applications. Linux scales from small devices to large servers, allowing portability of source code between systems. However, it is only through using Linux distributions that conform to the Linux Standards Base that this portability of source code can be guaranteed.

**1024.03: Servers**

**1024.03.01** Systems and/or projects providing servers shall adopt any of the following as best befits the function of the server:

**1024.03.01.01** Microsoft Windows

**Strategic** (continued)

*Server operating system with wide product support and an established user base.*

**1024.03.01.02** Linux distributions that conform to the Linux Standards Base

*Open source server operating system with an established customer base.*

**1024.03.02** The following operating systems shall only to be used if the mandated options above are not suitable for the required purpose:

**1024.03.02.01** Proprietary Unix

*Widely used to support legacy systems and high end requirements with a large and established user base.*

**1024.03.02.02** Bespoke/Specialist for small, high-end requirements

*Bespoke/specialist servers that offer particular features relevant to specific MOD requirements. These OSs should only be used when such requirements fall outside the scope of the more widely adopted servers listed.*

*Comment:* If the server is to provide proprietary network services for MS Windows client machines then MS Windows should be the OS of choice. If the server is to provide standards compliant network services then either MS Windows or Linux should be used. Unix should only be used when servers are required to provide either high throughput or high levels of availability.

**Deployed**

As for Strategic domain.

**Tactical**

**1024.04: Business and Workstation Clients**

**1024.04.01** Systems and/or projects providing business client devices shall adopt any of the following Operating Systems as best befits their purpose (see comment):

**1024.04.01.01** Microsoft Windows

**1024.04.01.02** Linux distributions that conform to the Linux Standards Base

**1024.04.01.03** Proprietary Unix

**1024.04.01.04** Bespoke/Specialist OS

*The decision of OS should be based on infrastructure requirements, application availability, environment and value for money.*

*Comment:* Preference should be given to MS Windows and Linux based systems rather than proprietary Unix or Specialist OSs.

**Remote**

**1024.05: Business Client**

**1024.05.01** Nothing is mandated in this area as the operating system is usually integrated with the client device (see comment for recommendation).

*Comment:* The choice of remote business client OS will largely be determined by whichever OSs have been accredited for connection to the strategic business system. It is recommended that devices are chosen such that the OS products are limited to the following: Microsoft Pocket PC, Palm OS, Symbian, and Linux.

**1024.06: Small Form-Factor Devices in Tactical Domain**

**1024.06.01** Remote Tactical devices are highly specialised and no single OS can cover all requirements. The OS shall be any the following:

**1024.06.01.01** Microsoft Pocket PC

*Pocket PC is widely supported on COTS handheld devices but lacks multi-user security capabilities.*

**1024.06.01.02 Linux**

*Linux is less widely used in handheld devices used but is capable of supporting multi-user security requirements.*

*Comment:* Linux should be preferred when large amount amounts of OS customisation is required. When customisation of the OS is required appropriate IPR should be acquired to ensure the future maintainability.

**1024.06.01.03** Bespoke/Specialist - these shall only be used where specific requirements cannot be met by off-the-shelf OSs.

*Bespoke/specialist OSs that offer particular features relevant to specific MOD requirements, where such requirements cannot be met by Pocket PC or Linux.*

## Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all MOD projects (and their suppliers) that provide Operating Systems on any device, including clients, servers and small form factor devices.

## Procedure

Not Applicable.

## Relevant Links

JSP602: 1037 - GII Engagement

A glossary of terms and abbreviations used within this document is available here.

Instructions on how to read a JSP602 leaflet are available here.

## Compliance

| Stage | Compliance Requirements |
|---|---|
| **Initial Gate/DP1** | MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s) as required. |
| **Main Gate/DP2** | MOD Projects shall reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the system, equipment or application they are procuring or updating. |
| **Release Authority/DP5** | MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance with standards shall be presented; sources of evidence may include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities. |