CLIENT & SERVER HARDENING POLICY

Contents

1 Overview

Client and server hardening is the process of developing and implementing configuration settings with good security properties to minimise vulnerabilities and to protect clients and servers from attack. It is a critical aspect of IL7's information security, ensuring that all ICT devices, end-points, hosts and communications facilities are operated in accordance with business need and are, as far as is possible, not vulnerable to compromise.

Most systems; software; and hardware, as delivered by manufacturers and resellers, are configured for ease-of-use, by default, and not necessarily for security. In-order to meet IL7's need to protect the confidentiality, integrity, and availability of its systems and information assets, systems; software; and hardware may need to be reconfigured to a secure standard.

Risks to IL7 if clients and servers are not appropriately hardened may include:

- attackers exploiting bugs in software that have not been patched.
- an attacker gains access to information they are not authorised to see.
- an attacker takes advantage of unnecessary user rights or privileges on a device/system.
- an attacker exploits unnecessary functionality that has not been removed or disabled.
- an attacker connects to unauthorised equipment that is then able to compromise information or introduce malware.
- an attacker creates a back door to use in the future for future exploitation.

1.1 Purpose

This policy defines the requirements for client and server hardening in IL7 so that all clients and servers are secured in line with the needs of IL7 and best practice (such as NCSC Cyber Security standards). This includes all user and client end-points; physical and virtual host servers; and communications equipment used to store; process; or transfer information, including metadata.

1.2 Scope

This policy applies to all clients and servers owned and used by IL7 including all end-points, hosts: servers both physical and virtual; and communications equipment used to store; process; or transfer IL7 information, including metadata.

1.3 Applicability

This policy applies to all IL7 staff, service providers and contractors who are responsible for developing, implementing, and managing clients and servers that interact with IL7 information, including all user and client end-points; physical and virtual host servers; and communications equipment used to store; process; or transfer information, including metadata.

2 Client & Server Hardening Policy

2.1 Policy and Controls

This policy is written to ensure that the outcomes of the following Cyber Security Principles are met:

- SP06 Operational Security (Ref [1])
- SP07 Secure Development and Configuration (Ref [2])
- SP09 End User Devices (Ref [3])
- SP11 Core System Protection and Separation (Ref [4])

This policy is one of several that are required to support the principles above.

This policy supports the following NIST controls, which are detailed in NIST Special Publication 800-53 (Ref [5]):

AC-8	System use notification
AC-11	Session lock
AC-12	Session termination
CM-5 (3)	Signed components
CM-7	Least functionality
CM-11	User installed software
MA-3(4)	Restricted tool use
MA-4(4)(b)	Authentication / separation of maintenance sessions
SC-2	Application partitioning
SC-7	Boundary protection
SC-7(12)	Host-based protection
SC-41	Port and I/O Device Access

2.2 General Requirements

Management shall ensure that:

Policy ID	Policy Requirement
2.2.1	All clients, servers and networking equipment used to store; process; or transfer information, including metadata, belonging to IL7 are configured by suitably qualified; trained; and security cleared personnel.
2.2.2	All secure build profiles are managed in accordance with the Configuration Management Policy (Ref [6]) and the Change Management Policy (Ref [7]).
2.2.3	Through-life IT Health Checks, Penetration Tests, and/or regular automated vulnerability scans are performed against all networked devices in accordance with the Security Testing Policy (Ref [8])
2.2.4	All assets are patched, tested and maintained in accordance with the Software Maintenance Policy (Ref [9]). This should include processes to assess, test and implement patches and ensure that software and hardware remains within vendor support.

2.3 Device Configuration

System Designers and System Administrators shall ensure that:

Policy ID	Policy Requirement
2.3.1	All clients, software, servers and networking equipment are configured with the principles of least privilege, need to know and the minimisation of attack surface (e.g. removing unnecessary functionality, removing unused accounts or privileges etc.).
2.3.2	All clients, software, servers and networking equipment are configured in line with the Build and Configuration Standard (Ref [10]).
2.3.3	All default passwords on clients, software, servers and networking equipment are changed to align with the requirements of IL7 Password Policy (Ref [12]) prior to use.
2.3.4	Host based boundary protections, including firewalls and anti-virus software, are implemented on clients and servers. [NIST SC-7 (12)]
2.3.5	Any deviations from approved builds are justified, documented and approved with GRA.
2.3.6	Any new secure baseline build profile for all systems and components, including hardware and software is documented, and approved by GRA.
2.3.7	Once configured, all devices are regularly tested to prove the integrity of the build and to identify and remediate vulnerabilities. See the Security Testing Policy (Ref [8]) [NIST CM-07]
2.3.8	All new clients and servers, are registered in the asset database with: • Date of configuration. • Date of last configuration test. • Date of next configuration test. Anticipated decommission date if appropriate.
2.3.9	All functionality or software that does not support a use or business need is removed or disabled.
2.3.10	Systems are configured using supported software. This includes versions of operating systems, web browsers, and applications that are vendor (or community) supported.

Policy ID	Policy Requirement
2.3.11	Technical controls are in place to prevent the installation of unauthorised software or change the configuration of devices. [NIST CM-5 (3), CM-11]
2.3.12	Maintenance of devices and their configuration is restricted to authorised administrators. [NIST MA-3 (4)]
2.3.13	Maintenance sessions are separated from other network sessions by physically separated communications paths or logically separated communication paths based upon encryption. [NIST MA-4 (4), NIST MA-4 (6)]
2.3.14	User functionality, including user interface services, is separated from information system management functionality such that management related functionality is not presented to non-privileged users. [NIST SC-2]
2.3.15	Clients and servers only connect to external networks or information systems through managed interfaces consisting of boundary protection devices. [NIST SC-7]
2.3.16	Physical ports on devices are locked down to only those required for the device to function and configured to only grant access to authorised devices. For example, by locking down USB ports to accept only pre-authorised USB devices. This In high threat environments this may be achieved by physically removing/disabling access ports. [NIST SC-41]
2.3.17	Changes shall not, without an explicit business reason and risk balance case: • Enable peripheral devices and removable media access; • Introduce unsupported software. • Increase privileges of the user. • Increase privileges of an administrator. • Disable any security enforcing function. Reduce the level / degree of audit or logging/

3 Exemptions, Exceptions and Breaches

3.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, please refer to the exemptions and exceptions policy (Ref [13])

3.2 Breach of Policy

IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in IL7 Disciplinary Procedure.

Breaches of this Policy by a third party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third-party service provider and/or the cancellation of any contract(s) between IL7 and the third-party service provider.

IL7 will refer any use of its IT resources for illegal activities to the Police.