Guidelines for Securing Leased Computer Hardware

Version 1.1

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: June 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	October 2017
1.1	MoTC logo changed	June 2018

Table of Contents

Introduction

The Ministry of Transport & Communication (MoTC) has issued the National Information Assurance Policy (NIAP) V2.0. The policy is mandatory for compliance by the government sector and strongly recommended for the critical sector organizations.

In line with the objectives of the Cybersecurity Department of MoTC, to drive the adoption of NIAP, this document is a step in this direction to help agencies put in adequate security controls on leased computer hardware.

Audience

Any organization that intends to use leased computer hardware.

The term Computer hardware includes desktops / laptops / servers / any processing unit and peripheral devices such as printers / Multi-Function Devices, Network devices etc.

Guidelines:

The following guidelines provide guidance to organizations that use or intend to use leased computer hardware within their organization. The guidelines ensure that any potential risks related to confidentiality, integrity or availability of the organization's information; and arising out of the use of leased computer hardware are adequately mitigated.

The security controls are spread across a typical life cycle of a leased computer hardware.

Procurement Phase:

1. Know your requirements:
    a. The organization should clearly identify their requirements within the RFQ / RFP.
    b. The requirements should include hardware, software requirements, business use, specific features (that you want and do not want), security and compliance requirements etc.
2. The client should define a service level agreement that clearly reflects its service level / availability requirements and communicate it to the vendor through the RFQ / RFP.
3. The vendor's proposal evaluation by the client should lay due emphasis on the supply chain assurance. These include:
    a. Trustworthiness of the vendor and their capability to stay in business (especially for long-term leases).
    b. Their presence in the local market and their experience in delivering the services requested by the client.
    c. References provided by the vendor should be vetted

4. The vendor should sign a NDA with the client that automatically covers all staff that provide service to the client. Q-CERT provides a sample NDA Template on its website.
5. Any disagreement on the terms of SLA by the vendor; should be communicated and agreed with the client during the technical discussion phase.
6. The client should ensure that signing of NDA and conformance to SLA is part of the vendor's proposal evaluation.
7. The client should ensure that the warranty / extended warranty / maintenance support proposed by the vendor conforms to the requested SLA requirements.
8. The contract with the vendor shall clearly specify penalties and legal action (if any) for the breach of NDA and SLA by the vendor.
9. The vendor should clearly document and present its procedures for media sanitization and media disposal in accordance to the NIA Policy.

System Delivery Phase

1. Computing devices (PCs, workstations; servers and network devices etc.) can be prepared in multiple ways for deployment. As much as possible, the organization should standardize on the configuration and the method of deployment to ensure consistency. Clients should provide the vendor with standard image of the operating system and required applications or a standard specification sheet clearly identifying the model numbers, version details of the firmware, software and any other application as applicable.
2. The hardware provided by the vendor should conform to the requirements prescribed by the client. This should be established through a formal Acceptance Test plan covering on a minimum:
    a. Standalone Product Testing: Before the product is connected to the client's production network:
        i. Ensure that any firmware / software used in the hardware is licensed and legal; to be used by the client.
        ii. Ensure that only Whitelisted Software (software approved by the client); is installed on the hardware.
        iii. Ensure that the hardware / software including third party application (if any) installed on the hardware is patched and Up to Date.
        iv. Conduct a vulnerability assessment on the hardware to ensure that no known vulnerabilities exist and / or the hardware meets the minimum baseline security requirements of the client.
    b. Integration Testing: After the product is connected to the client's test and development network.
        i. Maintain an inventory of all computer hardware deployed to the client's site or network.
        ii. Ensure that the computer hardware is classified; in accordance to the NIA Policy and considering the business information that it will store and process.
        iii. Change default local administrator password. Only the client administrator should know the local administrator password.

iv. Ensure that the hardware is hardened (as per the client's requirements) and is configured with specific security and application programs as applicable and as requested by client. E.g. End point protection client, encryption / DLP clients etc.
v. Ensure all applications installed on the hardware are patched and up-to-date at time of commissioning.
vi. Conduct a vulnerability assessment on the hardware to ensure that no known vulnerabilities exist and / or the hardware meets the minimum baseline security requirements of the client.
vii. Any exceptions to the standard procedure or Baseline Security Requirements or the client's specification; should be clearly documented in the Desktop Acceptance report.
viii. Prior moving the hardware to the production environment / network, the client should sign off the System Acceptance Report.

3. Responsibilities:
    a. The client should document and identify the responsibilities concerning the maintenance of the desktop.
    b. There should be clear delineation of work where multiple parties are involved.

Production Phase

1. Establish a process between the client and the vendor to report and resolve any issues / problem with the computer hardware as agreed with the client. The client should document all such information in a central repository to monitor the SLA governing the computer hardware.
2. Establish a process to ensure that any updates or bug fixes; are immediately communicated by the vendor and made available to the client and fixed as per the established division of responsibilities.
3. The vendor should schedule monthly / quarterly health check of the hardware.
4. Establish a process to ensure smart monitoring of the hardware; any potential issues that may affect the life / performance of the hardware are fixed prior causing a system outage / business disruption.
5. Any hardware / storage part; that is moved out of the clients place (for repairs, upgrade or return at end of lease) is treated in accordance to the media sanitization / disposal policy as prescribed in the NIA Policy.
6. Any temporary replacements; provided as an alternative replacement should be treated as a new device and adhere to this guideline in its entirety.
7. In case of a loss or theft of device, the client should report to the concerned authorities as per the organization's internal procedure, the asset register should be updated and a Risk assessment be conducted to assess the impact of loss / theft specifically in terms of information loss / theft. Where possible and as applicable all hardware procured should have controls such as remote wipe, encryption etc to protect against such threats.

Glossary

Client	Any organization that uses or intends to use leased computer hardware
Computer Hardware	Any computer hardware device, peripheral, network device etc leased by the client
Organizations	Any business organization including government / semi-government agencies, commercial organizations etc
Vendor	Leased computer hardware provider