Information Technology Equipment Life Cycle
February 26, 2021

Public Act 166 of 2020, Sec. 829*:*
Sec. 829. The MDTMB shall provide a report that analyzes and makes recommendations on the life-cycle of information technology hardware and software. The report shall be submitted to the Senate and House of Representatives standing committees on appropriations subcommittees on general government and the senate and house fiscal agencies by March 1.

Definitions

Life cycle: The period of time during which information technology hardware and software remains useful to the state.

Refresh rate: The planned rate of replacement for information technology hardware and software.

Background

Industry Lifecycle Practices

- PC hardware: Industry experts favor a four year life cycle for desktop PC's with a three year life cycle for notebooks. The State has implemented a four year on-site warranty for both desktops and notebooks. Units can be purchased or leased. Some agencies are keeping devices into the fifth and sixth years as the Department of Technology, Management, and Budget (DTMB) provides security patches and virus updates while software support remains available from manufacturers. Longer cycles may leave hardware out of warranty and unsupported; sub-optimize worker productivity; or present budget problems when market forces create an episodic need for a wider impacting change.

- PC software (operating systems and utilities): Upgrade operating systems strategically, remaining on supported releases of software, generally the current version or the current version minus one.

- Number of vendors (Dell, HP, Lenovo, Microsoft, Apple, etc.) supporting the organization: Typically, two to three vendors for each segment of asset category, such as desktops or servers. This practice assures that the state can continue to incent competitive pricing.

- The Governmental Accounting Office (GAO) stated that they do not have an official position, but the common federal practice, observed informally among agencies, is a three-year replacement cycle.

Security Issues

Eight major security issues support shorter life cycle replacement times for desktop and notebook computers:

1. Manufacturers constantly release patches to the firmware of their equipment to make sure it complies with the latest regulations and cybersecurity threats. When hardware reaches its End of Life (EOL), it may no longer receives those important updates. This means any new malware or cybersecurity exploits that are developed after your

hardware enters its EOL phase will have a much easier time infiltrating your systems, and may even be built specifically to exploit those weaknesses. This leads to a risk of system compromise via e-mail, instant messaging, or web browsing malware is greater with outdated hardware, operating system software, or application software.

2. The longer that you use hardware that is past it's warranty date, the more likely it is that you're going to run into incompatibilities that hurt your business. These incompatibilities can occur between hardware devices, as well as between hardware and software applications, which makes locating and remediating them very difficult.

3. Replacement parts for equipment that's reached its end of life phase gets exponentially harder and more expensive. In many cases, you're left with no other option but to pay for second-hand parts that come with no guarantee they're going to last or function correctly when they're first installed. This drives up the cost of your maintenance, and intensifies the instability in your systems.

4. Outdated hardware systems are vulnerable to attacks at sign-on and may not support current malware detection and remediation software.

5. Older systems do not support current security administration and authentication functions.

6. Security and vulnerability patches are often no longer available for older systems.

7. Older operating systems often do not provide the necessary tools to identify and remedy system compromises.

8. The overall security risk for older systems is increased due to a lack of available technical support and defensive measures.

State Lifecycle - Current Status

- All Executive Branch PCs are running the Windows 10 Enterprise 64-bit operating system, with some allowed technical exceptions (~5% of total systems).

- Currently 66% of deployed Executive Branch PCs are notebooks to enable a mobile workforce.

- Standard desktop, notebooks and tablets are purchased with four year on-site, Next Business Day (NBD) warranty with defective media retention.

- The average age of deployed PCs is 2.6 years. Still it is not uncommon for desktop workstations and printers to be used past their warranty period. Currently 14% of PCs are beyond their factory warranty.

- The State continues to move to a mobile environment at a rapid pace. The State has established mobile device standards and mobile application development standards to support the mobile worker environment.

- The most common reason for desktop equipment replacement is to support new applications and programs that require equipment with additional memory and faster processors to adequately meet customer expectations. The second leading reason for equipment replacement is to assure that security updates and application patches remain available and current. Desktop hardware is not yet being replaced at a rate that shows an average four year lifecycle across all agencies.

Lifecycle Recommendations

Leverage Existing Equipment

To leverage existing equipment, the state has established standards for usage and lifecycle based on the following user categories:

High-performance workers (power users): Users with compute-intensive or graphics-intensive applications and/or those that use large data sets in spreadsheets and/or databases such as software developers, graphic designers, or computer-aided design (CAD) engineers**.**

Mobile workers: Notebook/Tablet users who work outside the traditional office environment as much as 80% of the time. They tend to carry their notebooks most of the day and will often work in many locations including their vehicles and customer offices.

Day-Extenders: Notebook users whose systems tend to stay docked in the office the majority of the time. These workers typically take their notebook to other state offices for meetings or take their notebook home in the evening or weekend for extended projects and productivity.

Fixed-function or task-based workers: Workers who focus on very limited, specialized tasks such as claims processing. The performance demands of these applications do not change rapidly as these applications tend to remain in use longer than commercial office productivity applications.

Recommended PC Refresh Rates

- The recommended use per model is four (4) years (based on analysis of industry and government practices).

- The recommended on-site warranty period is four (4) years (keeps machines under warranty during useful life).

- The recommended time period for removal of desktop equipment from service is four (4) years (parts/patches no longer available).

- An exception process to these standards has been established by DTMB.

- DTMB will review the lifecycle refresh recommendation every year based on budget conditions and other impacting issues.

- DTMB will investigate new technologies and market directions to make recommendations for change as needed.

Desktop Salvage Process

The industry experts' reports indicate that PCs currently being deployed are sufficient for mainstream users for four years. However, as workstations age they can be transferred to workers needing less computer capability. Current State practice is that as new equipment is implemented, the older equipment is redeployed to another business unit. Redeploying desktop equipment is widely done across all state agencies.

- Usable desktop equipment is returned to the DTMB Depot to be re-distributed within the agency or reissued to other state agencies as needed.

- Obsolete equipment is properly salvaged through a contract with a Michigan electronics recycling company.

- The State's salvage and asset recovery programs are certified as zero land fill programs.

Recommended Average Server Refresh Rates

The industry typically depreciates servers over three years. However, pursuing a server replacement based solely on a financial depreciation schedule can cause unnecessary work. The server refresh rate in the state has a longer life cycle based on both financial depreciation and useful life.

- The State continues to pursue a virtualization strategy and cloud computing strategy which significantly reduces the need for physical servers.

- Most hardware vendors commit to five years of parts availability for servers; therefore, the State purchases five year on-site server support for servers supporting office functions in remote offices. These devices are also protected by uninterruptable power devices that are kept under the same warranty period.

- The goal for application servers kept in the Data Centers is a four year lifecycle. However, due to financial constraints, the State has the option to purchase five year warranties to extend the useful life when appropriate.

Recommended Software Replacement

The State maintains a technology roadmap for its business environment to match short-term and long-term goals with technology solutions. So while the latest release of operating system software is purchased with desktop and server equipment, it is also common practice to delay upgrading to a new release of software until after it has been in use in the private sector for a period of time to avoid unforeseen software problems. At the same time, the state makes every effort to change or upgrade the software to remain within the general release support cycle of

the manufacturers, and before software becomes unsupported. Software that is used beyond its supported life greatly increases the risk to the State of productivity loss, loss of vendor support, and vulnerability to malware or data security breaches.

As servers and PCs are purchased, the state typically licenses the newest operating system with downgrade rights to the current-minus-one version. This allows the state to plan migrations and have the necessary licenses available when the migration is made. Migrations to new operating systems are only to general release versions, never to beta versions, and will only be done after the industry has fully tested the newly released operating system and state applications have had time to test and validate operation on the new operating system.