



POINT OF SALE SYSTEMS

A Guide to Maintenance, Repairs, Upgrades, and Replacements

Brought to You by:

WORLDLINK
INTEGRATION GROUP

Table of Contents

- Hardware Maintenance** 1
 - Preventive Care, Maintenance, and Upgrades of Equipment 1
 - Average Lifespan of Equipment 2
- Software Updates** 2
- Most Common Problems** 3
 - Security Dilemmas 5
- Average Cost of Service** 6
- Average Time Needed** 6
 - Cleaning and Repairs..... 7
- Conclusion**..... 8



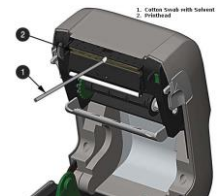
Hardware Maintenance

Point of sale systems are responsible for handling transactions, tracking inventory data, providing data for accounting, and securing sensitive customer information collected over the duration of a sale. These systems are crucial in the day-to-day processes of retail stores, restaurants, healthcare offices, entertainment venues, educational institutions, grocery stores, and any other customer-centric business. The data that these systems collect is analyzed by management, supply chain operators, and marketing teams to boost efficiency, tabulate accurate cash flow, and encourage growth in sales while minimizing loss. So, keeping these systems running efficiently and securely is vital to the success of most businesses. Point of sale systems will require regular maintenance, repairs, and replacements. The following manual will serve as a guide for management and IT teams looking to keep their point of sale systems running optimally.

Preventative Care, Maintenance, and Upgrades of Equipment

Tips for preventative care:

- Train employees on proper use and cleaning of equipment
- Regularly clean monitors, wipe down keyboards, dust the CPU, and wipe printer heads
- Run system scans on a regular basis
- Inspect cables and power cords for wear and tear
- Backup important files daily



What routine maintenance should be implemented?

POS systems need to be examined for out of date and/or faulty internal components such as memory cards as well as external hardware like pin pads or customer-facing displays. These devices may break down and cause errors in the system, which can render the entire system useless until the component is fixed or replaced. It is also likely that businesses will need to upgrade pin pads, credit card readers, keyboards, printers, and other peripherals for aesthetic appeal as well as functional efficiency.

Is it necessary to upgrade to mobile point of sale systems?

Many restaurants and retailers are opting to utilize tablets and/or handheld devices in tandem with their legacy point of sale systems to increase efficiency and create an engaging experience for customers. Mobile point of sale (mPOS) systems are beneficial for many businesses, especially those with large sales floors, but they are not an absolute necessity for most, if any, business.

If your company decides to integrate mPOS, the devices will need to be well-maintained, frequently scanned for viruses, and synced to the back-of-house system

through a secure network. If the devices are used by customers, they should be mounted or encased in a way that prevents theft and damage from occurring. It is important to treat the mobile devices with as much –if not more –care as their traditional counterparts to maintain efficient and secure synchronization with your legacy point of sale systems.

How will the chip and pin payment mandate tie into my current system? What updates will my system need? What components will need replacing?

Traditional point of sale payment terminals are not equipped to read and process the chip-enabled credit cards, which means businesses required to accept EMV-compliant payments as of October 1, 2015, will need to completely replace card readers and/or pin pads with devices that are compatible with chip and pin technology. Additionally, software may need add-ons or upgrades to integrate these new payment terminals into the POS systems. This can be an expensive and time-consuming project and should not be put off until October of 2015. Business owners should start planning for –and implementing –the necessary changes now so that there is time to run updates, spread out the cost over several financial periods, and test the new systems with time to resolve any issues that may arise.

Average Lifespan of Equipment

What is the average lifespan of a point of sale Central Processing Unit (CPU)?

The rate at which technology advances often leads to an early exit of hardware, but the systems can easily last upwards of 7 years in the presence of careful equipment handling and regular maintenance. This, of course, assumes that there is no system tampering, water damage, or other physical destruction to the hardware.

What is the average lifespan of peripherals?

Generally, peripherals such as keyboards, receipt printers, and handheld scanners last an average of 5-7 years depending on where they are located, the frequency of use, and the care that they receive.

Of course malfunctions, damage from employees or environmental factors, and equipment negligence will drastically decrease the lifespan of any hardware component of a POS system.

For a more comprehensive list on the average lifespan of POS hardware, click [here](#).

Software Updates

POS operating systems (OS) require a little more attention and more frequent updates than network hardware, due to their role in security and system efficiency. Minor improvements and adjustments are constantly made to point of sale software and require almost continual updates to maintain optimal functionality and security. The longer a system goes without upgrades and attention, the longer the list of accumulated exploits to which it may be vulnerable. This being said, it is important to set up your system to automatically monitor security threats, system errors, and possible upgrades. Whether this is done by an external source or your own IT department, the system should be programmed to

alert key players in your business to ensure any problems that arise are dealt with immediately.

More frequent updates and continual maintenance of operating systems can reduce the need for large-scale upgrades of major software components.¹ Large-scale upgrades can:

- Be extremely costly
- Require time-consuming testing
- Lead to additional staff training
- Result in a significant amount of time installing and deploying the software

How often should updates be run?

A general guideline is to run internet-based or cloud-based updates on a daily basis, with manual updates completed as is necessary for your particular software. This depends on the frequency in which your operating system requires such updates. Monitor this on a consistent basis and set up your system to alert you of any new and/or urgent software.

When should I upgrade my point of sale software?

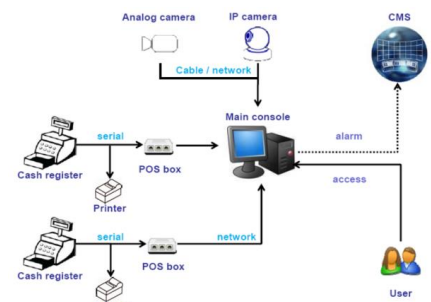
There is no standard timeframe as to how long a system should run on a specific software platform, but with the rapid rate at which technology advances, it is good practice to evaluate your current systems on an annual, if not semi-annual basis. The most common reason a revamp of software would become necessary is if the current application no longer meets the needs of an organization or the security has been compromised and/or lacks optimal effectiveness.

Most Common Problems

What are typical issues that arise with point of sale systems and how can they be resolved?

- Network connection errors
 - Unable to process non-cash payments
 - Failed connection to mobile POS devices
 - Failed synchronization to back-of-house server
- Outdated or malfunctioning equipment
- Compromised or out-of-date software
- Peripheral failure causing system malfunctions
- Central server memory and/or hard drive failure

Network connection errors can be caused by a plethora of problems and diagnosing these issues can be complex and tedious. See Worldlink's [Manual on Maintenance and Repair for Network Infrastructure](#) to learn what to do if connection issues arise.



¹ <https://www.techsoupforlibraries.org/cookbook-3/maintaining-and-sustaining-technology/replacing-and-upgrading-technology>

Outdated or malfunctioning equipment can cause slow payment processing speeds and inaccurate data collection or fail to work altogether.

Before discarding the hardware:

1. Check to make sure that all cables are undamaged and connected properly.
2. Scan system for viruses and run any necessary updates of software.
3. If all connections are in order and all peripherals are working properly, but the problem is not resolved, reboot your system.
4. If this does not resolve the problem and there is no visible physical damage a technician can test your systems. They can utilize an external computer to review the system's operating data and/or open up the CPU of a POS terminal to see if a component such as a memory card, circuit board, or cooling fan is the culprit or if the entire system has reached its end of life.

If a peripheral device, such as a printer, keyboard, or scanner is malfunctioning or connected improperly, the main terminal may cease to function² as it is setup to follow a certain protocol that it may not complete without all connected devices functioning properly. If the central system has been tested and is running properly, attempt the following:

- Power off, wait 10 seconds, and reboot peripheral devices
- Check all cables/connections to the POS terminal
- Try connecting another terminal's peripheral to the malfunctioning system to see if the currently connected peripheral(s) is/are broken or malfunctioning



If you are alerted of an issue with the memory, you may need to clear space by removing unnecessary files or transferring older, but valuable, data to an external hard drive or cloud storage system. Hard drives may also become corrupt or overtaxed and need to be scanned, wiped, and/or replaced.

Continual monitoring and maintenance of all hardware can mitigate the majority of the above-mentioned risks and prevent time-consuming and often costly restructuring and/or overhauls of network systems.

² http://www.ehow.com/info_8091513_point-sale-problems.html

Security Dilemmas

A major concern for any business using POS systems in its day-to-day operations is the risk of viruses, malware, and hackers corrupting the system. These attacks can destroy your systems and provide access to customers' payment information and personal data, as well as company files that are crucial to the success of the business.

To mitigate the risk of these threats it is important to run scans on all devices on a regular basis and educate your employees on the proper procedures of processing payments, logging in/out of the system, and correctly shutting down systems at the end of shifts. All access to the personal payment data should be password protected and only key players should have knowledge of the password to sensitive information on your servers.

It is also wise to use tokenization and data encryption to make any information vulnerable to digital theft useless to any hacker who manages to invade your system. Data should be stored on services or external drives that are not connected to the main network and follow all [PCI Compliance requirements](#).

Many systems will now be required to take chip-enabled cards which further protect customer data, but the technology is not infallible. As there are no guarantees in protecting a point of sale system, the best approach to security is a proactive, preventative maintenance plan rather than a reactive one. However, it is important to have a plan in place in case your system does fall victim to a breach.

Tips for Preventative Maintenance:

- Change passwords once a month
- Make sure anti-virus software is up-to-date
- Run full system scans weekly
- Maintain the most sensitive data on a separate server
- Backup new files on a daily basis and run a complete backup weekly
- Protect every connection with passwords
- Use data encryption and tokenization
- Ensure PCI compliance

Steps to Take if an Attack Occurs:³

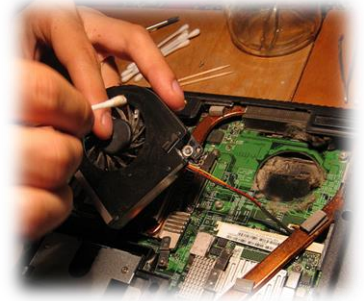
1. Identify the attack
2. Quarantine the infected servers, computers, and devices
3. Disinfect the network by isolating infected files, disconnecting from the Internet to prevent additional hacking, attempt to remove any viruses from the corrupted files, and then reboot the system.
4. Disclose the attack to proper channels (seek advice of legal and PR teams)
5. Re-secure network with new passwords and training of employees on security best practices

³ <http://www.seculert.com/blog/2013/07/network-compromised-5-critical-steps-to-handling-a-security-breach.html>

Average Cost of Service

Fees for service, repairs, and installation of replacements or upgrades can vary quite a bit. Fees for service usually run about \$65 to \$85 per hour, so since most hardware replacements will take about an hour (as seen in the table [below](#)), the cost per replacement per contractor will be around \$75 on average, excluding travel and related expenses. Of course, more terminals and/or the need for several contractors will rack up higher fees.

As for cost of equipment, this amount can vary quite a bit based on hardware specs, the brand being purchased, how many terminals are needed, and the number/type of peripherals associated with each. The *average* cost of hardware for a complete point of sale station that includes a computer, receipt printer, scanner, and cash drawer is around \$2,000 to \$3,500.⁴

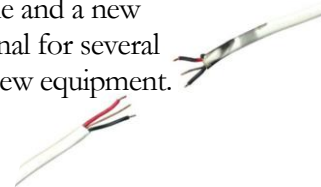


Average Time Needed

Basic cleaning of the external components of the POS system using compressed air to remove dust and debris takes roughly ten minutes per POS computer. If the internal workings of the CPU need to be cleaned, one technician can usually handle taking apart, cleaning, and reassembling the point of sale computer within an hour. This time frame may be extended if issues arise when the system is powered back on or if a mechanical error is observed when the casing is opened up.



Checking for loose or frayed cables that connect the CPU to peripherals like cash drawers and receipt printers is also a relatively quick task consisting of a few minutes per POS terminal. This means your business is not likely to be disrupted or impacted unless a cable needs to be replaced or if the wire is irreplaceable and a new peripheral device needs to be installed. This can disrupt use of the terminal for several days if spare parts are unavailable, requiring a purchase and delivery of new equipment.



⁴ http://www.armsys.com/art_purchase.html

The following table includes average times needed to handle replacements, additions, and troubleshooting for a basic point of sale service:

Service Task	Average Time Needed
Monitor replacement	1 hour
Cash Drawer Replacement	1 hour (more if <i>entire</i> POS must be taken apart to access/replace the cash drawer)
Accessing and then Reconnecting Cable to Cash Drawer	1 hour
Keyboard/Mouse Replacement	30 minutes
Customer-facing Display Replacement	30 minutes
Receipt Printer Replacement	30 minutes
Pin Pad Replacement	30-45 minutes
Memory Card Replacement/Addition	1 hour (varies depending on <i>how</i> technician must access the memory component)
Price Scanner Replacement	30-45 minutes
Troubleshooting	1 hour (this varies depending on the complexity of the dilemma and various other factors)

Replacing components of existing POS terminals, adding more terminals in a store, or replacing old systems can take hours or days depending on the scope of the project.

- Connecting new peripherals to current systems will likely take less than an hour to power up the device, connect the peripheral, configure the peripheral to work properly with the system protocol, and test the process.
- Installing new terminals can take several hours depending on various factors such as:
 - Routing for new cabling to establish network connectivity, which may take the longest amount of time depending on how difficult it is to run the new cables
 - Whether or not there is room at the cash wrap for another register or if an additional cash wrap is needed
 - What it takes to prepare the new or existing cash wrap for an additional register and peripherals (i.e. drilling of holes for cable access, mounting a pin pad/scanner, etc.)
- Replacing old systems- this is typically quicker than installing an entirely new terminal because connectivity and space should already be available. However, if the network connectivity needs are different, if the new register has a larger or smaller footprint than the old one, or if it has different peripherals, the install may take longer. This also holds true if old peripherals need to be removed, existing holes need to be patched, or other modifications to the cash wrap are a necessity for supporting the new system/peripherals.

Cleaning and Repairs

Equipment should be regularly wiped down and/or air-dusted to ensure unwanted debris does not interfere with the copper connections and other sensitive equipment. From time to time it is necessary to do a more thorough cleaning, which may require unplugging cables and/or dismantling the point of sale CPU as well as ensuring the equipment is reassembled properly and all connections to the network are reinstated securely. This may require hiring an outside resource if an internal IT team is not available or trained on POS hardware and network connectivity. The amount of time it takes to wipe down equipment and blow out any micro-debris will depend on how many systems are in need of cleaning. Generally, a basic cleaning of a system by employees will take less than an hour, but a building with numerous POS terminals will likely require a bit more time and/or manpower.

As for repairs, these should be done as soon as an issue arises and can vary based on the equipment that needs to be replaced. The timeframe is also dependent on whether it is just a component of the system that needs replacement (often requires less time) or if a full swap-out is required.

Conclusion

Staying on top of basic maintenance, repairs, upgrades, and replacements will help point of sale systems last longer and mitigate the risk of unsecure systems. The benefits and long-term savings accrued from basic service far outweigh the minimal costs of annual and/or semi-annual cleanings and repair. Of course, there is no guarantee that routine maintenance will prevent hacking, equipment malfunctions, or unforeseen damage from customers or employees, but they do help to reduce the potential for minor problems that can lead to costly overhauls. Consulting a third-party service provider with experience and knowledge of POS systems can add tremendous value to your current system by expanding the life of your technology for greater return on investment. After all, you wouldn't drive a car for 30,000 miles without ever once getting an oil change or tire rotation, right?

For more information on Point of Sale system installation, purpose, and modern uses, visit our [original content page](#) or check out our [Twitter](#) page or [Scoop.it](#) feed.

