Best Practices for Asset Management

MORSE WATCHMANS
think inside the box.

What is Asset Management?

Every kind of organization and business has valuable and sensitive items which need to be kept out of the wrong hands. From tools to weapons to mobile devices, every asset used by an organization presents a risk profile.

Not only is the theft of valuable items a financial loss, but also many mobile devices now hold important data including intellectual property and personal information. Mobile devices can be used by hackers to break into a network, install malware, steal data, hold access for ransom and infiltrate every other server and device on the network.

Overall, the risks presented by small assets are tremendous and must be addressed as part of the organization’s overall security plan. This whitepaper will detail best practices for securing, controlling and managing your assets to minimize the possibility of theft, damage, misuse or other risks.

"When it comes to valuable assets, it's not enough to place items together in a single locked closet or drawer."

The Need for Accountability

From the smallest family-run shop to global enterprises, businesses and other organizations have a greater need for accountability than ever before. Many businesses have stockholders who expect transparency on every vulnerability and potential loss, and who will take action if they are not satisfied with the level of risk mitigation. Other organizations are subject to strict compliance regulations for a range of functions including security and the protection of high-value assets.

For every type of business, liability exposure is significant; one serious case could put you out of operations permanently.

When it comes to valuable assets, it's not enough to place items together in a single locked closet or drawer. Not everyone who uses a 2-way radio should have access to firearms, or cash drawers. Each asset has its own set of permissions, which may change by the day or even by the hour. Locked doors and drawers are also far too easy to breach.

An employee who has been terminated must also immediately lose their access to whatever valuable assets they previously used on a daily basis. Simply asking them to relinquish keys is inadequate, since keys can be copied before they are handed back.

Spotlight by Industry

The number and variety of assets that every industry uses and must keep secure is vast. What presents the greatest challenge is this: not only must these items be protected from theft and other risk, but they must also be fully accessible to the specific individuals who have the authority – and the need – to use them to do their jobs every day.

Retail:

- Intercom system headsets and beltpacks
- Cash drawers
- Mobile checkout systems

Law Enforcement/Courts:

- Weapons
- Visitor valuables
- 2-way radios

Offices:

- Data storage devices (hard drives)

Airports:

- Expensive tools

Hospitals:

- Weapons (for gun-free hospitals)
- Laptops/tablets for EHR (electronic health records)
- Medications

Gyms:

- Guest valuables
- Mobile phones that need to be charged

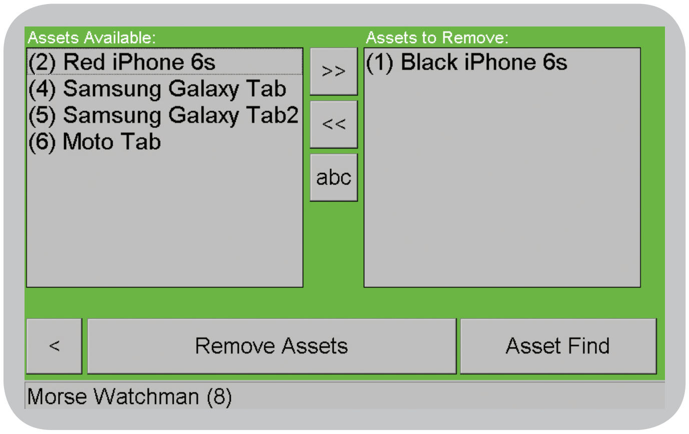
Corrections:

- Visitor valuables

> *"An asset control system is a cabinet with individual lockers, each requiring specific access permission in order for any individual to have authority to open any given locker."*

Even authorized individuals could potentially leave the premises with items they have either forgotten to return or intentionally kept after their workday ended.

By following best practices for asset management, you can protect against all of these serious challenges and help your organization focus on what is most important to maintain their core mission.


Assets Available:

(2) Red iPhone 6s
(4) Samsung Galaxy Tab
(5) Samsung Galaxy Tab2
(6) Moto Tab

Assets to Remove:

(1) Black iPhone 6s

Morse Watchman (8)

Best Practices for Asset Management

Your valuable assets should be stored, secured, tracked and accounted for individually in order to protect them from risk. The best way to manage this is through the use of an automated, electronic asset control system.

An asset control system is a cabinet with individual lockers, each requiring specific access permission in order for any individual to have authority to open any given locker. Each time a locker is opened, the system logs the information including the identity of the person, the time, any relevant notes entered into the system and the asset entered or removed.

If the individual does not have authority to remove that asset at that time, the system can deny them access to the locker by keeping it locked. If they remove a different asset other than the one they are authorized to remove from a locker, the system can instantly and automatically notify authorities of the removal.

By integrating asset management systems with other business systems, a wide range of other capabilities are enabled. For example, it is possible to have an individual's authority to remove assets terminate automatically when their employment ends. Or, if someone has failed to return an asset to the cabinet, they can be flagged and denied access to other areas of the facility.

Making an Asset Management System Work for You

There are many different ways to set up a system of permissions using a system of lockers to manage assets. You need to consider the requirements of your organization and learn the capabilities of the system you choose.

You may be able to configure your system in a variety of ways based on your needs. Some of the possibilities may include:

Individual Ownership of Lockers

Each locker in the system can be assigned to a specific individual. This is ideal for work environments when the same personnel are on site regularly and need a secure space to store small personal items or weapons – especially if they occasionally need to leave those items overnight or when they are away from the workplace.

Temporary Ownership of Lockers as Needed

All lockers in the system are available for use by any authorized individual on a first-come-first-served basis.

"To follow best practices for asset management, each valuable asset should be RFID-tagged so that it becomes an identifiable data point."

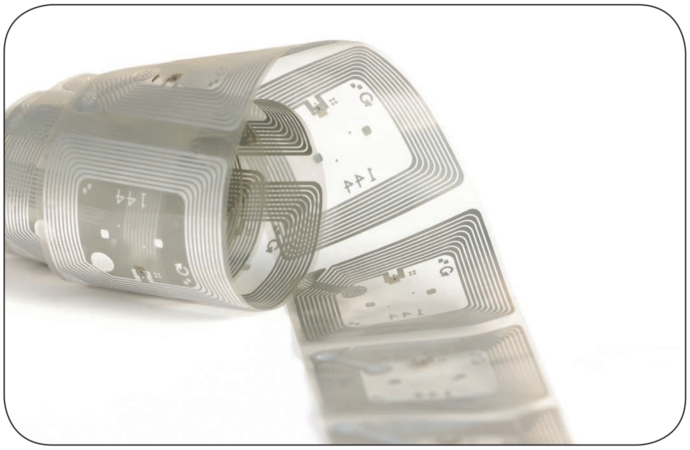
If there are multiple shift-workers who come and go frequently on differing days, this is an excellent way to minimize locker needs while ensuring enough space for all who need it. It also works well for temporary visitors or guests who need a safe space to store items.

Assets Assigned to Specific Lockers
When there are highly valuable individual assets that are shared among employees, it can be a useful practice to keep each in its own locker.

RFID Tagging

One effective technology that helps enable accountability and accuracy in asset management is the use of RFID tags.

Radio Frequency Identification, or RFID, uses electromagnetic radiation in the radio range to identify the number of a tag which is in close proximity to the reader. Whenever an RFID tag comes within range of an RFID reader, it is detected and read. Commonly in use in retail store tag systems and electronic toll collection systems, RFID is a highly cost-effective technology for tagging individual items so that they can be identified and tracked electronically.



To follow best practices for asset management, each valuable asset should be RFID-tagged so that it becomes an identifiable data point. This way, the system always knows which assets are in use and which are locked away safely.

RFID tagging helps with accountability in numerous ways, including:

- Identifying which device is located in which locker
- Tracking who has removed or returned each device, and when it was removed
- Recognizing assets when returned or removed
- Auditing by device or by user for a better view of device usage
- Discovering which devices are available for use
- Restricting access to specific devices based on user, time or other criteria
- Ensuring items are returned to a specific locker when required

To learn more about RFID technology and how it can help you manage assets, **download our whitepaper**.

Leveraging Technology Capabilities with Asset Management

Once you have made each asset into a data point and placed them in a networked locker system with controlled access, there is a world of information that becomes available that can be used for business and security purposes.

Taking advantage of these capabilities can turn your asset management system into an asset for business as well. Here are three features that deliver significant benefits to your asset management system:

Permissions
Specify for each individual asset who has the authority to use it. You can further qualify permissions to indicate time of day, day of the week or other conditions as needed. To

> *“To further increase security, you can configure your system to require more than one individual to present credentials to remove and/or return a specific asset.”*

further increase security, you can configure your system to require more than one individual to present credentials to remove and/or return a specific asset.

Notifications

Management or other authorities can be automatically alerted via text or email under a range of conditions; for example, if a particular weapon is removed from the cabinet, or if it is not returned by a certain time. This enables quick response and remediation in situations when it is needed.

Reporting

Knowing who is using assets, and when, can provide a wealth of business intelligence. Take some time to familiarize yourself with the standard reports that are built into your asset management software, and you will see the types of insights that could be valuable to the organization.

You should also be able to customize your reports further, so that they provide exactly the information you need most, and to use the system’s automated features to deliver them on a timely basis to those who will find them useful.

Networking

For larger organizations, distributed enterprises or campus operations, it makes sense to use a number of networked asset cabinets placed at locations convenient to the people who will be using them. In this situation, you should consider for each individual asset whether you

USB Charging for Mobile Devices

Consider these two facts: our population is on the go more than ever before, and they are more dependent on their mobile phones than ever before. Put the facts together, and you get a lot of people who need to charge their phones, all the time. That’s why you will occasionally see a phone, left untended, plugged into an outlet at an airport, shopping mall or other public place by its owner who is desperate to charge it. This is clearly a high-risk move; even in an office, leaving a phone untended can temp thieves.

Additionally, for organizations who have company-owned devices that are used only during the workday and secured at night, these devices need to be kept charged so that employees don’t arrive to pick up their work tools and find them unusable.

For these reasons, it’s an important part of asset management best practices to secure devices in a location where they can charge while they’re waiting for their next use.

> *“Requiring authentication of identity via fingerprint reader, facial or iris recognition is the best way to validate with the highest certainty that the person presenting credentials matches the identity on those credentials.”*

want it to be returnable to any cabinet in the system or be limited to certain locations. Each offers advantages based on the needs of the users.

Networking the system enables central management of the database and cabinets and makes it possible to access information from anywhere.

Security

Using an asset management system obviously increases the level of security for all the items stored inside. As the administrator of the system, you can further customize this by cabinet, by user or by asset using a number of features.

Credentials and Biometrics

When selecting the system you are going to use, look at the different types of access requirements you can deploy. There are keypads for pin numbers, scanners for ID cards, prox devices and more. For the most valuable assets you can consider biometrics. Requiring authentication of identity via fingerprint reader, facial or iris recognition is the best way to validate with the highest certainty that the person presenting credentials matches the identity on those credentials.

Two-Person Authentication

Casino compliance regulations require two people from different departments to log in to remove keys for cash boxes. This is an excellent way to raise the level of security for removing an asset, and should be configurable on your asset management system.

Notification

While this feature has been mentioned already, it is worth repeating here as it provides another layer of security for certain sensitive assets such as weapons. Alerting security management every time a weapon is removed, along with information about the person who removed it, can be vitally important to preventing incidents.

Conclusion

Your organization, your workforce and your customers are more diversely distributed than ever before. To make sure they have the tools they need, and to provide them with secure spaces in which they can have peace of mind, asset management is a must.

It is also an essential part of your business operations to make sure you minimize the risks presented by all of the tools, mobile devices, weapons and other valuable assets you may have on the premises at any point.

By following the best practices advocated in this whitepaper, you can accomplish all of these goals and keep your focus squarely where it should be – on serving your partners, guests, patients, customers and personnel, and on accomplishing your organization’s core missions.