A Managers Guide to Secure Disposal of Electronic Devices

CellPhone Bank DATA SECURE

www.Data-Secure.org

866-290-7864

Why Should I Be Reading This Guide?

The lost and found department for many hotels, amusement parks, transportation companies, and entertainment venues, is, on many occasions, the responsibility of an already overtasked department head or manager. Generally included with security, human resources, or housekeeping, rarely is lost and found a department all its own.

This guide is intended to help lost and found staff create a policy that securely deals with the unclaimed electronics in their possession. It is well known that smartphones, tablets, laptops, and other portable electronic devices, contain a treasure trove of data that, in the wrong hands, could harm the original owner. As a member of the lost and found staff, it is incumbent upon you to act in a manner that protects your customer's privacy and the reputation of the company.

"It is incumbent upon you to act in a manner that protects your customer's privacy and the reputation of the company."

Why Does My Company Need a Disposal Strategy?

If you're like most people, your smartphone, tablet, and laptop hold your entire life. We use them to schedule appointments, send e-mails, take pictures; we even pay our bills and manage our finances by using our electronic devices.

Now, imagine you lost one of them...would you panic? Most likely the answer is yes, not necessarily because of the cost of replacing the gadget, but because of what it contains…. your life, in little bits of electronic data. In fact, a recent survey of smartphone users ranked losing their mobile computing device as being more stressful than losing their wedding ring (77% vs 55%).

Now think about the devices that are under your care and keeping in your lost and found. Would the owners of those devices want you to protect their personal data? YES! This is especially true when a device is unclaimed. You MUST dispose of unclaimed devices in a manner that protects the privacy of the device owner.

Most smartphones hold a wealth of information about the user. Should a phone fall into the wrong hands, this data is remarkably simple to retrieve. A Federal Reserve survey found that 51% of smartphone owners used mobile banking last year. According to the same survey, 38% of smartphone owners had not password-protected their devices, and 32% had auto sign-in for banking and financial websites. ***Disposing of a device without properly erasing user data is tantamount to handing control of your customer's bank account to an absolute stranger.***

This document will guide you through the process of evaluating your current unclaimed electronics disposal method. We will

delve into the basic technical requirements your process should meet and how you can insure your disposal method protects your customer's information and your reputation.

What Does Secure Disposal Entail?

There are two basic components to a secure disposal program. First, all data must be permanently erased from working devices. Second, any devices that cannot be erased must be recycled in a manner that protects the data from being recovered at a future time.

Permanent Erasure – Erasing devices is not simply a matter of performing a factory reset. The factory reset process does not necessarily erase the data. For a video demo of just how easy it is to recover data visit https://www.data-secure.org/android-factory-reset.

> "The factory reset process does not necessarily erase the data."

To ensure the data on devices is not recoverable, each device must be erased in compliance with minimum industry standards. Available 3rd party, licensed erasure software can ensure your devices are erased to current industry standards. Below is a list of the minimum standard by device type.

iOS – Cryptographic erase
Android – Character Overwrite NIST SP 800
Flash Memory – Character Overwrite DOD 5220
Hard Drives – Character Overwrite DOD 5220

Additionally, 3rd party verification ensures the integrity of your erasure process. This requires a licensing agreement with a reputable erasure software provider.

Environmental Standards - Not all devices can be adequately erased. Some will not power on, are damaged, or are obsolete. These devices must be recycled by a certified R2 recycler. An R2 recycler strictly follows both environmental and security standards for the electronic recycling industry.

What Should I Look for in a Third-Party Processor?

A charity's staff may be expert at counseling victims, or providing food to the hungry, or shelter for the homeless, but very few have the skill, capabilities, or resources to permanently erase private data from an electronic device. Law enforcement may accept lost and found devices, but that does not mean they have the skill or resources to adequately erase the data they contain. Regardless of who is processing devices on your behalf, be certain to get satisfactory answers to the questions below.

> "If your processor relies only on factory resetting devices, find a new processor!"

A. Who is processing the devices?

When donating, first determine who is doing the actual processing of the devices. Most charities simply pass the devices on to a third party to process and sell. If your agreement is not with the third party, should a data breach occur, you could be held liable for any damages sustained by the original owner of the device.

Ask the following of the 3rd party processor:

a) What erasure standard does the processor use?

   Most organizations (non-profit and for-profit alike) simply use the built-in factory reset, or hard reset as some refer to it, to clear devices. As the video, referred to above, proves, factory resets don't always delete personal data. Make certain the processor you choose adheres to the minimum standards listed above. Otherwise, you leave yourself open for liability.

   If your processor relies only on factory resetting devices, find a new processor! Regardless of the good they may accomplish, they are leaving your company, and you, unnecessarily exposed to potential liability.

b) Can your processor prove the devices are being erased properly?

   Many organizations that process simply assure you that the devices are being erased properly. That's why 3rd party verification is important. Without it, you must take the word of the processor. However, with it, a qualified, 3rd party software provider will confirm the device has been erased. Most processors do not use 3rd party software because of cost; licensing can cost tens of thousands of dollars per year or more.

"...a qualified, 3rd party software provider will confirm the device has been erased. "

c) Does the processor operate a secure facility?

   Most facilities have basic security like an alarm system, dead bolts on the doors…etc. However, since portable electronic devices are just that - portable - there must be increased security inside the processors' facility.

   i. Background Checks - A background helps your company identify applicants that have a criminal past. While someone with a past may qualify to work in other capacities, they should never have access to devices that contain your customer data.

   ii. Secure Processing Area – The processing area must be secure, with locking doors, and

accessible only by staff that have a legitimate reason to enter. Doors from the secure processing area must **not** open to the outside of the building.

iii. Security Cameras – Good surveillance, whether live monitored or recorded, discourages theft and pilfering. Since the processor will have memory cards and thumb drives that can easily be slipped into a pocket before erasure, cameras in the entire facility are a necessary deterrent.

iv. Alarm Backup and Monitoring – The facility's security alarm must be monitored. In addition, it should have a battery powered, wireless backup that allows it to continue to operate if the phone lines or power is cut.

d) Do the processor's policies ensure security?

Extra care must be taken when hiring and managing employees, and when handling customer shipments. Policies that will ensure your customers data will be protected, while under the control of the processor, are imperative. Below is a list of minimum policy requirements that should be in place.

i. Personal items that can be used to steal or pilfer, such as jackets with pockets, lunch boxes, purses, backpacks…etc., should not be allowed in the processing area.

ii. As shipments are received, they must be immediately secured in the processing area. Shipments should never be opened outside of the secure processing area. If devices are removed by the processor, or their representative, are they properly secured before removal (i.e. – are boxes taped, are they being transported in a vehicle that can be locked…etc.)

iii. Only necessary staff, who have had a background check, should have access to the secure processing area. It should be clear **who** is authorized to enter the secure processing area, and **what the consequences are** for unauthorized entry. Visitors should not be allowed in the secure processing area.

iv. Devices that have not been erased should not be taken outside the secure processing area.

B. Does the processor have a professional liability insurance policy?

   Mistakes happen. Your processor should have a liability policy that covers them if they are negligent in the service they provide and one of your customers is harmed. They should have no problem adding your organization as an additional insured on the policy.

C. Does the processor use a certified R2 electronics recycler to recycle broken or obsolete devices?

   Proper disposal of broken or obsolete devices goes beyond the environmental aspect. Using a certified R2 recycler ensures that devices, that cannot be erased, are destroyed.

What Now?

The way you choose to dispose of guest property has a bearing on how your company is viewed by the outside world. Showing as much concern for your customer's privacy after they leave your property, as you did while they were your guest, builds trust.

A worldwide survey, conducted by security software company Gemalto, revealed that 64% of consumers say they are unlikely to do business with a company who experienced a data breach, and 75% believe that companies do not take data protection seriously.

Handling unclaimed devices is more important than ever before. Trust is essential in building relationships, and for companies that hold customer data, this is especially the case. Unfortunately, data breaches are having an impact on consumer trust and loyalty. Now, the perception of the way you handle guest data, influences consumer decisions.

Take the necessary steps now to protect your company's reputation far into the future.