1. **Waste and Data Security**

In today's economic world, information is the lifeblood. It travels with a mouse click or a screen tap. Data processing is a topic that affects almost every firm in almost every industry in almost every country.

As a result, data security, also known as information security, is a major aspect that businesses must take seriously in order to safeguard themselves, their clients, and their interests.

Criminals, on the other hand, have advanced along with technology. Data thieves abound, and they're not the ones swinging from a tightrope suspended from the ceiling trying to grab a hard drive in black leotards. These criminals steal critical information using both digital and physical techniques, and they work around the clock from anywhere (sometimes even from your own staff).

So, how does this relate to recycling? Improper disposal of spent assets is one of the most prevalent and straightforward ways for these unscrupulous actors to obtain sensitive information. We at GLEC are here to ensure that this does not happen and that you and your data remain safe.

**What is the definition of data security?**

It is the process of safeguarding data and other sensitive information throughout its lifecycle from illegal access, theft, and corruption.

Data comes in numerous shapes and sizes, but it is your most valuable asset for several reasons. In today's digital age, data is at the heart of everything. How you safeguard information is known as information security.

There are numerous tools available to protect your data. Continue reading to learn more!

**How to protect your data?**

Your information security measures may differ depending on the sort of data you process and the nature of your organisation, but there are still best practises to be aware of and adopt in your company.

* Secure
* Back up
* Training

**Secure Your Data**

The actual security measures you've put in place to keep criminals from gaining access to your data. The following are examples of security protocols.

**Encryption:**

Tokening is a term for data that has been encrypted with a password. If a specific key is supplied, data is only accessible or viewable.

**Erasure**

When you no longer require the obtained information, properly remove it so that it cannot be stolen.

**Masking**

Masking is the process of only presenting sections of data sets while masking others, ensuring that the integrity of the entire data set is not jeopardised.

**Multi-Factor Authentication**

A split of encryption that necessitates the use of multiple passwords or other keys. i.e., in addition to a password, a bio authenticator such as a fingerprint or retinal scan may be required to gain access to information.

**Back-Up**

It's not just about keeping your data out of the hands of criminals; it's also about securing it. Computers break, disasters strike, viruses infect computers, and so on. There are a plethora of ways in which your valuable data can be destroyed.

As a result, you should make a backup of your data. A wise strategy to back up data is to use offsite server storage, such as a cloud system.

Physical copies, such as flash drives and discs, are less secure and not as suggested as cloud-based storage methods, but they are still helpful.

**Training**

While technology is critical for information security, the human factor is just as important, if not more so. An business can have all of the best data security policies available, but they're useless if employees and other members of the organisation don't follow them.

Organizations must provide regular training to employees so that they not only understand the importance of these security measures, but also how to get personnel to sign in and stay compliant.

Finally, data security policies must adhere to industry best practises, just as enterprises must adhere to industry best practises to achieve success in their work and with clients. Keeping up with the latest best practises and ensuring that staff employees are trained in them helps to ensure that protocols are followed and sensitive information is protected.



Hackers and data thieves are a genuine issue nowadays, therefore data security should be one of your top priorities.

**Most at Risk**

While any firm that handles data is theoretically vulnerable to data theft, the medical industry, aside from the financial sector, may be the most vulnerable. Cybercriminals are very interested in medical records, especially because there is so much information that can be accessed.

Medical documents can cost up to $60 per asset on the dark web, according to Formassembly.com. That may not appear to be a significant cost on its own, but when you consider the enormous volume of medical records available, it becomes clear.

If you work in the medical industry, make sure you follow all of the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Provisions to limit health-care fraud and abuse, establish industry-wide standards for health-care information on electronic billing and other processes, and require the safety and confidentiality of protected health information are three of HIPAA's core concepts. The United States Department of Health and Human Services has more information about HIPAA requirements.

**What is the Purpose of a Data Security Policy?**

According to ConsumerAffaris.com, the Federal Trade Commission processed 1.4 million fraud reports in 2018, resulting in damages of $1.48 billion. According to the same group, there are an average of 5,233 attacks every month against networked and data-sharing devices.

So, what does this imply for you and your company? It implies that you must use caution. You and your firm could be held accountable for any losses clients or others suffer as a result of a data breach.

Unlike the European Union, the United States does not currently have a national standard for information security. The EU adheres to the General Data Protection Regulation (GDPR), which establishes data security policy and management standards for EU member countries (if your business does a lot of work in the EU, you will have to conduct yourself under these laws).

**Data Disposal**

During the disposal procedure, fraudsters have one of the best opportunities to obtain data. If obsolete computer assets aren't properly disposed of, fraudsters will be able to take your old items and steal whatever information is stored on them.

Before you try to get rid of any electronic assets, be sure you've deleted all of the data off of each one. This can be accomplished by a variety of methods, including disc clearing and degaussing.

At the end of the day, however, gadgets should not be thrown away. Just because the data on your computers and other devices has been erased does not mean that they may now be thrown away with other trash. It merely serves to protect your data from would-be hackers and data thieves; your materials are now ready for proper recycling. This is especially true in the healthcare industry.



Code and other sensitive information are as valuable as gold to a data thief or other type of cybercriminal.

**Hardware Disposal**

Aside from the environmental implications of throwing e-waste in the garbage with other things, data breaches are a significant issue that occurs more frequently than you may imagine. It's a burgeoning issue that's only going to become worse.

According to the National Conference of State Legislatures, at least 35 states and Puerto Rico have passed business e-waste legislation as a result of this. These rules force commercial or public bodies to completely erase their data. You could be held legally liable for data and privacy breaches if you don't prepare and recycle your unwanted and obsolete digital gadgets.

Each firm should have a data plan in place to cope with obsolete IT equipment and data. In terms of technology, "out with the old and in with the new" is what drives business.

However, disposing of assets and data in a responsible, safe, and ecologically friendly manner should also be a major issue.

**Need Help?**

If you haven't already discovered it, you can't just throw away your unwanted IT assets; they must be readied for disposal through sanitation or destruction. You shouldn't, and in some situations can't, throw out old technology.

Business electronics can pose as many issues as they can solve in today's technology-driven society. We can aid with liability reduction and the complete tech data recycling process if you need it.

[Recycle Pro](https://www.recyclepro.co.uk/) can help you with the processing and recycling stages of your hardware asset management process to ensure a smooth, ecologically beneficial, and secure flow.