

Secure circular services

Why recovering redundant assets helps to prevent cybercrime



Computacenter



Introduction

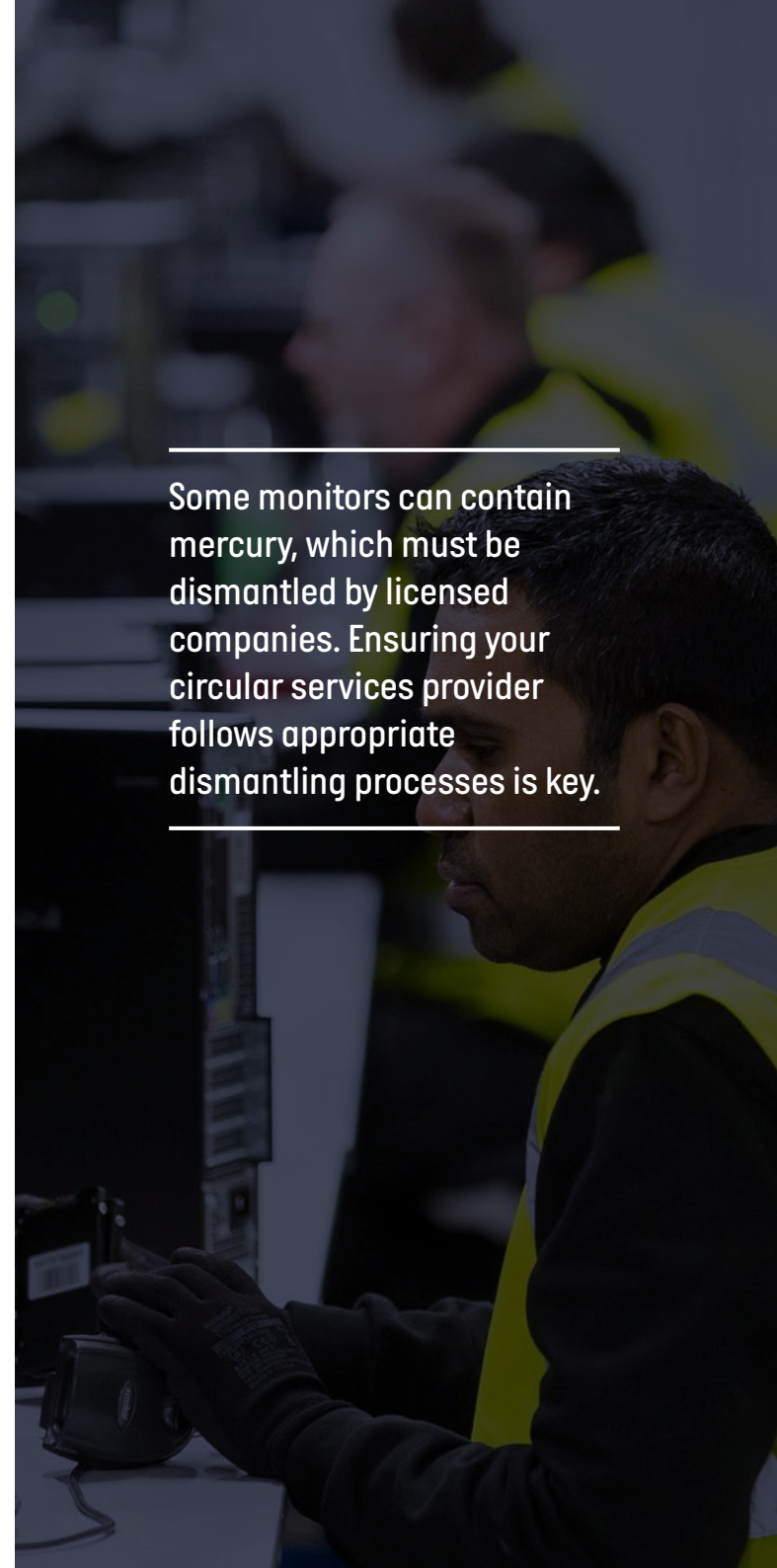
Organisations have evolved significantly in the last decade. Home and remote working, coupled with the adoption of cloud services, have created levels of flexible working that were once considered impractical. Whilst there is still debate as to the impact on productivity, it is clear that the modern workplace is here to stay.

This shift has been accelerated by several factors. Firstly, there is the vast increase in devices; gone are the days of a single, static desktop that the user had to travel to to use, and instead most enterprise users now work with a laptop, a smart phone and often also a tablet, all of which travel with them. Secondly, there is the growth in the adoption of cloud services and applications, allowing workers access to core systems from outside the corporate perimeter. Add the potential of AI and the increasing amount of automation, and it's clear that day-to-day user experience and worker flexibility has changed for the better.

Unfortunately, despite these improvements, there are some unintended consequences of greater worker flexibility and user experience. With the rise of cloud, AI, and automation there is now more data than ever before, and with the increased number of devices and the use of cloud services

there are now many more places where this data is both stored and accessed. Protecting access to this data and stopping it from being exploited by threat actors is a major challenge for most organisations, particularly given the advantage new AI-powered attack methods are bringing. Data is at the core of the infinite game between attacker and defender. For the attacker it is the means with which to extort financial gain or achieve geo-political advantage; for the defender, the theft or loss of data creates the risk of enormous financial and reputational damage. Therefore, organisations must take every precaution to protect their data, and this includes making sure that redundant and retired devices and technology are disposed of securely. Specifically, this means ensuring that data on redundant technology is sanitised before or during disposal and that it cannot be accessed by threat actors once it has left the organisational perimeter.

Some monitors can contain mercury, which must be dismantled by licensed companies. Ensuring your circular services provider follows appropriate dismantling processes is key.



Device disposal

Organisations, particularly large Enterprise-scale businesses, can employ thousands of people in office and administrative roles, many of whom use multiple devices. Devices in this fleet will reach a point of redundancy and need to be replaced due to their age, their performance, their inability to operate the latest versions of software, and the end of manufacturing warranty. All of these devices are highly likely to contain both sensitive corporate data and Personal Identifiable Information (PII) data, making them a significant risk to corporate security if not disposed of correctly.

In addition to end user devices such as desktops, laptops and phones there are many other office equipment technologies that can contain data that could be used by threat actors if recovered by them. These include devices such as cameras, printers, plotters, scanners, photocopiers and desk telephones. Many organisations do not realise that photocopiers and printers can contain vast amounts of corporate data in their internal memory. In fact, there have been cases where gigabytes of sensitive documents were retrieved from decommissioned photocopiers by interrogating internal memory, simply by using legal and affordable tools.

Beyond the office, redundant technology components found in data centers and machine rooms are also subject to the same challenges regarding data. These items include servers, routers, receivers, switches and bridges. They often contain encryption keys and certificates and separate storage components that may hold other sensitive data. Whilst manufacturer reset will help to render any data unreadable, there is a wide range of rigour dependent on the vendor which means that some reset capabilities will be less effective than others.

All of the above technologies incorporate data storage capability in the form of internal flash memory, Hard Disk Drives (HDDs), Solid State Drives (SSDs) and Hybrid Drives (HDD + SSD). Ensuring that data here is removed, sanitised and, sometimes in the case of HDDs, degaussed and even shredded, is essential before the technology is disposed of. SSDs are harder to sanitise than HDDs given that there is no single data erasure product that can operate across all brands. This is because each manufacturer develops Solid State memory in a different way, embedding their own software into the chip to control the mapping of logical addresses to physical addresses, and vice versa. A failure to consider how to sanitise SSDs before or during disposal can leave highly sensitive data accessible.

Technology disposition options

Whilst technology disposition strategies are driven in the main by a desire to support environmental objectives and recover a proportion of investment costs, the potential benefit to an organisation's security posture should not be overlooked. Regardless of the technology, secure disposal at the end of its first useful life is crucial. Failure to do so can lead to significant data loss, causing reputational and financial damage that outweighs any environmental or financial benefits from reuse or recycling.

As a consequence, when faced with the need to replace any of the devices previously described, most organisations will choose one of the following options:

Redeployment

Redeployment and reuse of existing equipment within an organisation can lead to considerable cost savings and environmental benefits. However, it involves ensuring data is sanitised before items are passed to new users, and the logistical challenges of delivering to multiple locations. The collection and subsequent redelivery of technology equipment also brings with it the risk of kit falling into the hands of threat actors.

Resale

Companies can choose to sell their IT equipment to a third party to recover some of their costs. This method can be cost-effective and environmentally friendly but carries a high risk of the device falling into the hands of attackers. As such it is essential that any technology being disposed of in this way is fully sanitised before being sold.

Donation

Donating IT equipment to a charitable organisation or non-profit can be a socially responsible method of asset disposition. However, it may require extra effort to ensure that the equipment is properly refurbished and meets the needs of the recipient organisation. Companies also need to consider several factors when choosing a donation partner, including the partner's mission, reputation, and its capability to handle IT equipment. As with resale there is also the same issue regarding the need to fully sanitise the technology before donation. It is also worth noting that many charities prefer to receive funds from resold IT equipment to put towards new – or new equipment bought from those funds – rather than receiving donations of technology that is already at the end of its first life.

Recycling

Recycling IT equipment can be an environmentally friendly method of asset disposition. However, it may require more effort and expense to properly recycle the equipment, and there may be concerns about the safety and environmental impact of the recycling process. As this method of disposal is usually undertaken by specialist third parties, ensuring that their security guardrails and sanitation processes are effective is critical.

Whichever method is chosen, it is important to remember that the devices have been used to access corporate systems and applications, involving the processing and storage of significant amounts of data. This data can include password information, PII such as credit card details or name and address, and sensitive corporate information. A failure to remove this data prior to, or during, disposal will pose a serious security risk to the disposing organisation and may breach local compliance laws and regulations.

Despite this risk, many organisations do not have suitable device disposal processes, and many devices will not be recovered or will exit an organisation without proper sanitisation and with little clarity as to how sanitisation will be undertaken by the disposal agent. The temptation to either redeploy or donate redundant technology, or offer it for resale, also creates a risk that threat actors will be able to access sensitive data that can be used to support future cyber attacks.



What are circular services?

Circular services (an alternative name for IT Asset Disposition or 'ITAD') are designed to help organisations realise the value of technology that is approaching the end of its intended first use.

They focus on the circular recovery and subsequent redeployment, remarketing or recycling of equipment to minimise the impact and demand on our environment, and in doing so they are also able to address the security issues discussed in this document. Circular services allow organisations to recover capital from their technology investments whilst reducing the rate of equipment turnover and subsequent environmental impact.

Services typically include secure collection, processing, and data sanitisation, with additional services around asset identification, audit and reporting. The most effective circular services organisations strive to deliver assured and certified services securely, sustainably, and with full compliance to relevant regulations and best practice. They also provide detailed asset-level reporting to provide end-to-end visibility and tracking of assets showing where and how they have been disposed of.

Circular services provide an essential service in a world of finite resources and are increasingly being used by organisations to further their environmental and sustainability strategies. However, they also play an increasingly important role in ensuring that organisations can meet their security compliance and risk management obligations.

Regulatory compliance

IT Asset Disposition is important for regulatory compliance because it ensures that companies conform to requirements and standards, particularly in areas such as data security and the disposal of electronic waste. Reputable circular services suppliers should comply with the following regulations:

WASTE ELECTRICAL AND ELECTRONIC EQUIPMENT (WEEE) DIRECTIVE

The WEEE Directive sets out standards for the disposal of electrical and electronic waste and aims to reduce the amount of WEEE waste produced. It encourages following the Waste Hierarchy, starting with the prevention of creating waste, followed by choosing to prepare WEEE for reuse, followed by recycling it, then using other methods of recovery, and finally disposing of it where all other options are not possible.

ISO 14001

The International Environmental Management Standard ISO 14001 demonstrates that a supplier has assessed the environmental impacts of its operations on the environment and is committed to monitoring, controlling and improving environmental performance. The standard requires legal compliance with environmental regulations.

ISO 27001

Certification to the international standard ISO 27001 demonstrates that security risks associated with a supplier's operations are identified, and mitigation controls in place. This includes site security and data destruction. The standard shows that legally compliant policies, procedures and security controls have been implemented and maintained, and people trained to use them.

GDPR

The General Data Protection Regulation (GDPR) is a regulation that governs data protection and privacy in the European Union. Companies must comply with GDPR regulations when disposing of personal data stored on their IT equipment.

Recommendations for device disposal and sanitisation

If data bearing surfaces are not treated properly, sensitive data may remain accessible. This could result in the following issues:

- Unknown whereabouts of sensitive data, which may contravene regulatory standards.
- Loss of control over information assets.
- Critical data could be recovered and used by ill-intentioned threat actors or competitors.
- Private or personal data relating to an organisation's customers or staff could be used to commit fraud or identity theft.
- Risk that intellectual property could be recovered and published openly, leading to loss of reputation and revenue.

As such, it is important that organisations develop a clear strategy to address both how redundant devices are prepared for disposal and how they are disposed of.

Preparation and sanitation


To best manage the risks associated with sensitive data held on storage media, organisations should:

- Invest in a process that enables the evaluation, categorisation, and assessment of data and its potential value outside their organisation.
- Baseline the cost of sanitation and secure disposal, and adapt budgets to account for it, for example incorporating it into planned procurement costs.
- Create a clear reuse and disposals policy, ensuring that there is complete clarity as to how, when and why redundant technology is sanitised and disposed of.
- Establish an asset-level inventory record of the technologies that have been deployed and retain the manufacturer manuals to ensure there is a guideline on how to sanitise media before shipping it to a third party.
- Keep a record of the lifecycle of storage media that covers what is it being used to store, where is it storing data, and for how long is it being stored.
- Always use trusted third parties for disposal and sanitation activity and make sure that they operate to recognised industry standards.
- Be sure to obtain data sanitation and/or destruction certificates from third party providers.
- Periodically test destruction and disposal processes and equipment to help verify that data is being sanitised appropriately.
- Before disposal, remove all labels or markings that indicate ownership of the device (or the nature of the data contained).

Disposal

The following cost and risk considerations can be used to help shape policy regarding the secure disposal of technology:

- Consider any obligations to comply with environmental policy (for example WEEE).
- Consider any obligations to comply with industry or government sanitation standards.
- Research the availability of disposition companies, assessing their services, disposal techniques, accreditations, security guardrails and their pricing schemes, and establish what happens to kit when it leaves an organisation.
- Consider the geographic distance from an organisation to the disposal site. Establish if supplier vans make stops en route to the disposal facility, and request information about how the risk of interception is managed - for example, using the 'two-person integrity rule'.
- Discover whether staff have the skills to decommission equipment on-site or to perform sanitation on some types of equipment before it is shipped to a disposal partner.
- Consider constraints around the redeployment, donation or resale of certain equipment.
- Establish how long to store equipment before accumulating a volume that is economically viable to dispose of – considering asset resale values and depreciation.
- Assess where your organisation is using cloud for data storage, and seek to understand what level of security is in place as part of the contractual obligations of the cloud provider. Establish assurance of what is contractually provided or consider implementing additional guardrails.



Some commercial and municipal incinerators can have cold spots inside, and data bearing surfaces can be inadvertently protected from heat by their casings. Assure yourself that any incineration facilities you or your circular services providers use can explain how they prevent a failure to properly incinerate data bearing surfaces.

How does Computacenter help?

Our Circular Services offering enables us to manage the recovery and redeployment, remarketing or recycling of equipment to minimise the impact and demand on our environment – and we do this worldwide. Our scale and capability allow organisations to recover maximum capital from their technology investments whilst reducing the rate of equipment turnover and consequent environmental impact; all while ensuring that data is secure and risk of data exposure during the disposition process is minimised.

Services are underpinned by secure collection, processing, and data sanitisation, with asset identification, audit and market-leading reporting delivered as standard. We deliver our services securely, sustainably, and with full compliance to relevant regulations and best practice. Detailed asset-level reporting provides end-to-end visibility and tracking.

Recovery

Once a device exists, it should be fully utilised for as long as possible to minimise its impact on the environment. Computacenter helps customers realise the most value from their used equipment with over two million items recovered each year.

We offer on-site decommissioning and data sanitisation services where required, helping our customers to manage risk and ensure protection from exploitation by threat actors. We collect devices from locations around the world, and securely package and transport them to a Circular Services Center for testing, assessment of device condition, and documented data sanitisation. Our technicians ensure any company asset labels and identifying markers are removed and that data is thoroughly sanitised. HDDs and SSDs that fail the sanitisation process are shredded before being recycled.

With over 30 years of experience in the IT Asset Disposition industry, our Circular Services teams can provide our customers with expert guidance on how to keep their data safe during the disposition process; and we have detailed knowledge of all makes and models of IT equipment that need to be processed and sanitised of data. Should new types of equipment require processing, we will investigate how best to sanitise them before we start processing.

Equipment is thoroughly audited, with records kept against each device to ensure full chain of custody from recovery right through to final disposition.

Following the technical processing of items, we prepare them for redeployment, remarketing or recycling.

Redeployment



Extend life

- Reusing devices is the best way to reduce environmental impact.
- We clean, reconfigure, and redeploy items back to our customers.
- This service ensures unused devices do not remain unsanitised.
- Over 70% of a device's carbon footprint comes from initially making and shipping it.
- Reusing devices saves money vs buying new, and avoids unnecessary carbon and water consumption.

Remarketing



Maximise value

- Surplus devices are recovered and assessed for reuse.
- Rehoming devices maximises their useable life.
- We provide an auditable record of assets having been sanitised before resale, evidencing data security.
- Our Buyback services enable customers to unlock residual value and ensure devices are reused.
- Value recovered can be used to fund new purchases, or for charity donations to aid in sustainability strategy objectives.

Recycling



Recycle sustainably

- Devices that no longer function or have become obsolete are recycled, with working components recovered.
- The priority is to maximise recovery of valuable raw materials, which are then returned to the supply chain for reuse, reducing the impact on our environment from mining new.
- Recycling ensures that sensitive data cannot be recovered by threat actors.
- Hardware is processed in accordance with all relevant legislation and recognised best practices.
- Asset-level reporting provides full visibility on material recovery data and outcome.

These services are underpinned by our world-class facilities in Braintree (UK) and Gustavsburg (Germany), supported by worldwide logistics and partnerships, ensuring we can provide services at scale and across all device types.

Customers wishing for a higher level of security can make the most of our Braintree facility and Global Control Tower, which is PASF and UK Government approved. It is the largest facility of its kind in Europe, with the capability to handle data up to Secret and occasional Top Secret classification.

Comprehensive services

Secure collection | 100% data destruction | Asset tracking
Workplace | Data Center | Networking | Security

A person's hand is pointing at a document on a server rack. The server rack has a sign that says "HEIGHT SUPPORT" and "CIRCUIT BOARD SIDE DOWN".

Data sanitisation

We offer a range of data sanitisation solutions, from on-site drive destruction through to wiping using Blancco software at our Circular Services Centers and partner sites. We can meet a range of national and international standards, in line with specific customer requirements. Standards adhered to include IEEE 2883-2022, HMG Infosec Standard 5, BSI-2011-VS and NIST 800-88, amongst others.

Reporting

Reporting with clear data provenance is critical to meet sustainability goals and for regulatory compliance. Computacenter's customers receive asset-level inventory reports and certificates of data sanitisation. Where recycling is carried out, certificates of HDD and SSD destruction are also available. These reports and certificates ensure peace of mind that data has been securely and effectively sanitised or destroyed. Our asset-level reporting allows our customers to clarify how each item has been allocated during the ITAD process. Customers can compare reports with their own asset management systems to ensure a correlation.

In addition, our customers receive regular environmental and financial reports summarising all service and asset processing activity. They highlight key environmental benefits – carbon reduction and water savings – achieved through:

1. Avoiding the purchase of new equipment via redeployment and remarketing
2. Recovering reusable raw materials from obsolete technology through recycling

Our Circular Services Centers

Inside our state-of-the-art Circular Services Centers, built specifically to manage the responsible recovery and recycling of IT equipment, devices are securely delivered, assessed, then actioned based on their health and age. Services are carried out at strategically located secure facilities to ensure that device and lifecycle management is always within reach, giving customers peace of mind about their assets, and the opportunity to reduce their environmental impact.

Selected certifications and governance

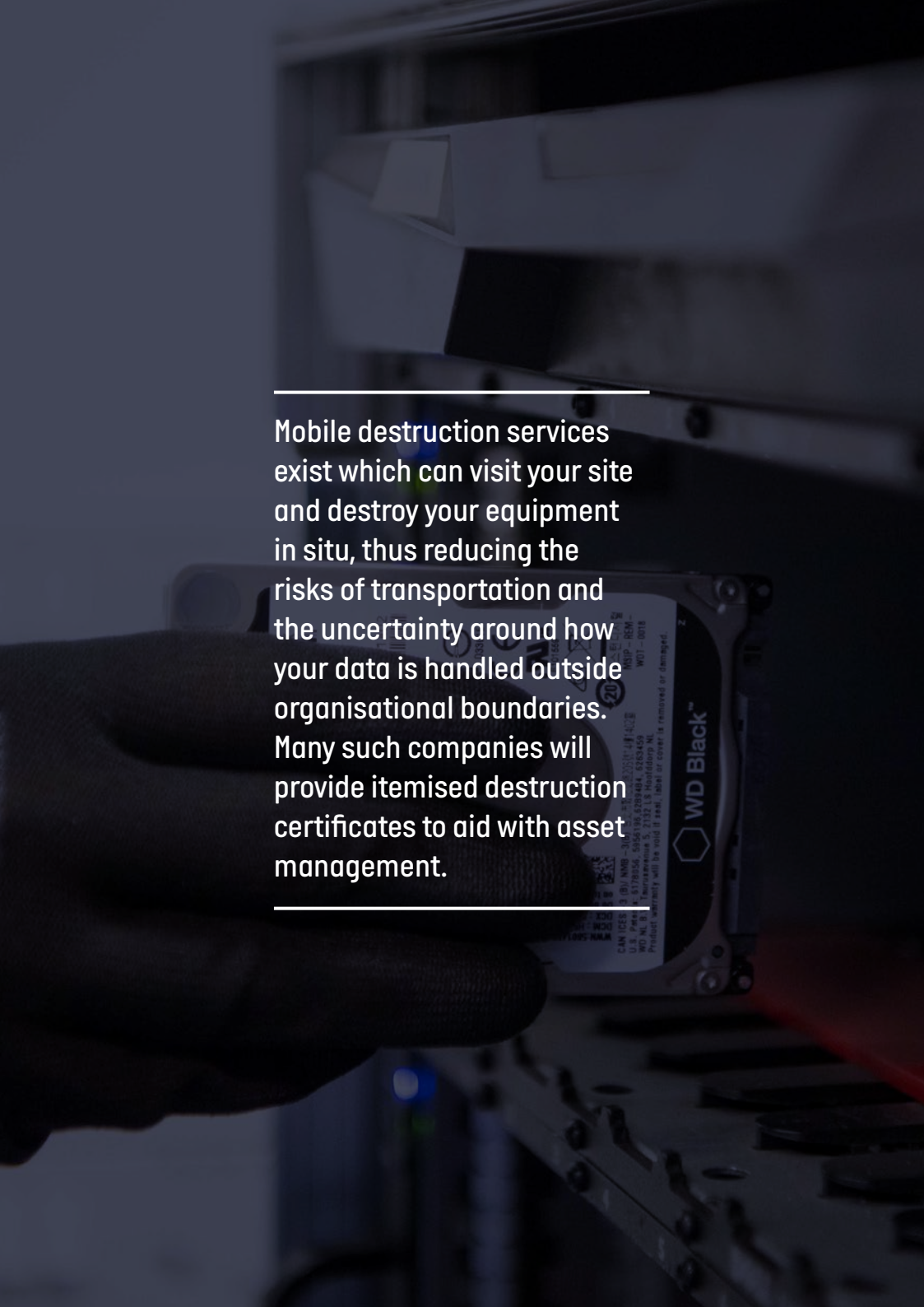
We monitor and audit our processes to ensure consistency and quality. In addition, we fully on-board and audit our partners, and we regularly shut down downstream recycling partner sites to monitor their processes specific to our customers' equipment and to ensure the accuracy of our environmental reporting.

Our target: to recover a device for every device we sell

Over two million items were processed through Computacenter's Circular Services business in 2023. Of these, around 775,000 were devices – PCs, tablets, switches, servers, monitors, printers and routers. In that same period, we sold around 4.7 million new devices. To achieve our target, we don't want to reduce the number of new devices we sell but want instead to grow the number of devices we recover.

By significantly scaling our Circular Services business we believe we can make a faster impact on helping our customers achieve their own sustainability goals, helping us build long-term trust and loyalty while also making a positive impact on the environment at the same time.

While we are committed to this goal, we will continue to ensure the safety of our customers' data when handling redundant equipment – without cutting corners.



Mobile destruction services exist which can visit your site and destroy your equipment in situ, thus reducing the risks of transportation and the uncertainty around how your data is handled outside organisational boundaries. Many such companies will provide itemised destruction certificates to aid with asset management.

In 2023, we:

Processed over

2 million

items

Redeployed

174,805

items

Remarketed

895,119

items

Environmentally recycled

967,970

items

Saving

119 million

litres of water, and

avoiding

117,000

tonnes of CO₂

Benefits

Choosing Computacenter as an ITAD partner offers a number of benefits:

- Organisations save by reducing the storage and maintenance costs associated with outdated or obsolete equipment.
- Asset disposition can boost revenue via reselling or repurposing valuable assets.
- Proper ITAD can reduce disposal costs by recycling IT equipment, which can help organisations avoid landfill fees and other disposal costs.
- ITAD can help organisations meet their environmental goals by reducing electronic waste, ensuring the safe handling and disposal of toxic substances and reducing their carbon footprint.
- Properly disposing of e-waste can also help prevent the release of harmful chemicals into the environment. Being environmentally responsible can have many benefits for companies, including reducing costs, improving brand image, and attracting socially conscious customers.
- By using Computacenter's Circular Services offering, customers can be reassured that disposal will add an additional layer of defence, closing a potential gap in data security.
- The service is highly secure and ensures that no valuable corporate information, asset labels and identifying markers, or PII data and passwords can be exploited by threat actors.
- As well as conforming to the standards mentioned earlier in this document, we hold certifications above and beyond the level of many other ITAD providers, including R2, CAS[S], and Cyber Essentials Plus.

Summary and conclusion

In a world of finite resources, where achieving greater levels of sustainability is an increasingly important corporate objective, deciding how to dispose of redundant technology is vital. Many organisations will look at options such as refurbishment, resale, donation, and recycling of their redundant devices as a way of meeting self-imposed targets and regulatory compliance.

Whilst these options are undoubtedly valuable in terms of social responsibility, a commitment to sustainable business, and will deliver some cost savings, they must be undertaken in the most secure way possible. With increasing amounts of data existing on more devices and more technology components than ever before, it is hardly surprising that it is the target of increasingly sophisticated cyber attacks.

Ensuring that this data is protected, and every effort is made to restrict access to it, must extend to include data held on redundant technology. As such, choosing disposal options that guarantee effective data sanitisation is critical, as is investing in new processes and policies that structure disposal planning and data sanitation best practice.

Computacenter's Circular Services functions are designed to address all of the above. With years of experience, a deep service portfolio and extensive accreditation, we partner with many global organisations to securely manage their redundant technology disposal needs.

To understand more about how Computacenter is delivering secure Circular Services for other organisations, please contact us at SecurityEnquiries@computacenter.com, or visit our [Circular Services webpage](#).

Let's talk

For more information contact us at SecurityEnquiries@computacenter.com, visit our website, or contact your Computacenter Account Manager.



Computacenter (UK) Ltd
Hatfield Avenue, Hatfield, Hertfordshire AL10 9TW, United Kingdom