WHITE PAPER: Data Sanitization for the Circular Economy

Revision 1.0, Version 1.0

July 2022

Author (s) :

Jonmichael Hands, Chia Network, Circular Drive Initiative

Fahmida Bangert, Iron Mountain, ITRenew

Luke Steck, Seagate Technology

Arie van der Hoeven, Seagate Technology

Brad Warbiany, Western Digital

Geoffrey Cottrell, Sims

Executive Summary

Most storage devices get destroyed at the end of first use due to security concerns. This eliminates the possibility of a circular economy because it prevents any further uses of the devices. Media sanitization is a well-researched and understood field, with a new international specification just released to address the modern methods and techniques to prevent unauthorized access to data. We present the use of “purge media sanitization,” which is the fast and secure way to remove all data on a device and enable second use.

Table of Contents

Table of Figures

Introduction,

The audience for this forward-thinking whitepaper includes major hyperscalers, technologists, product managers, and architects looking to tackle sustainability and circularity in data center equipment. The guide assumes basic-intermediate level knowledge and practice and relies on the reader's desire to move the needle towards sustainability and climate action in their respective roles. This guide benefits from peer review and suggestions, and we welcome your feedback. Varying corporate liability policies are out of the scope of the document, but the goal is to influence future policy based on facts about media sanitization and risk.

Background: Data security as a barrier to circularity

Technology is driving globalization and the available data about customers, products, and services. With this increased amount of data comes great responsibility, and every organization is liable to protect proprietary and personally-identifying information of their customers, products, and services. Losing data can have a moderate to severe primary impact (financial, reputational, and product development) and secondary impacts (decreased productivity, slow customer service, loss of customers, and reputation damage).

As a result, organizations go to great lengths to secure sensitive data, and fundamental to any cloud service provider's business is the customer's promise that their data is secure in the cloud. It is, therefore, common to physically destroy data-bearing devices (DBDs) such as hard disk drives and solid-state drives, despite advanced encryption and security features on devices and near zero risk of data leaks. Physical destruction, commonly including punching and shredding DBDs, eliminates the

ability to reuse the devices or makes it economically infeasible to recover sub-components, such as rare earth magnets.

Protection of DBDs via destruction becomes a great barrier to circular products and circular systems implementation in the value chain toward carbon emissions reduction for the planet. With the ultimate goal of reduction of environmental and toxicity footprint in mind, Circular Economy principles employ 'reuse, sharing, repair, refurbishment, remanufacturing and recycling' to create a closed-loop system, minimizing the use of resource inputs, and the creation of waste, pollution and carbon emissions.

DBD's contain rare earth metals, the manufacturing of which is a sizable source of Scope 3 emissions. When the DBDs are shredded, they create a great deal of e-waste, the long-term value of the DBD is lost, and the toxicity associated with heavy metals is directly released into the environment. There are methods and techniques to securely prevent access from data on a DBD, known as media sanitization, without physical destruction!

Today's common practice

It's essential to learn safe data handling practices and options. By understanding what steps to take, a functioning drive can be made safe for internal or external reuse, and a non-functional drive can be secured to make data unrecoverable. If you ask many people what they would do to sanitize their data, they may say, "just format the drive." If the drive is broken, they may say "I'll just dispose of it". In both cases they don't have enough knowledge to make an informed decision. There are different options for formatting a drive. Depending on the option utilized, data may physically remain on the drive. If the drive isn't working, there are also various forensic methods that can be utilized to recover data from both HDDs and SSDs. Data lifecycle management includes creating, storing, using, sharing, archiving, and finally, destruction. Destruction, in this case, is intended to prevent unauthorized access to the storage media, but destruction alone is not secure. There are secure methods of making data recovery infeasible, including encryption and sanitization capabilities built into the drives themselves.[See Appendix B]

Physical destruction processes also vary by the type and size of the drive being destroyed. In most cases today, the final process to destroy a defective drive will be shredding. The size of shredding required will depend on the type of drive. Platter-based drives will require less effort to break the platters into pieces, while chip-based drives will require a smaller shred size to ensure each part of the chip is damaged. There are other destruction methods that may be accepted as final destruction or as an interim method for transportation. Hard disk drives can be run through a degaussing machine, which uses magnetic energy to erase all data stored in the drive. Another method is crushing, which bends the body of the drive and deforms the spindle and platters. Chip-based drives are not susceptible to degaussing. However, crushing with a special spiked tool that damages each chip may be used. Shredding, which is still common practice, has actually been deprecated in recent specifications due to media density on hard disk drives - leaving small pieces of disks still with large amounts of potentially recoverable data.

Choosing a media sanitization method involves assessing the risk of the impact of data recovery with the probability and economic cost. Unfortunately, policymakers today have favored destruction, despite good evidence that the other best practices for media sanitization have a near zero risk of data recovery. What is needed is a specification that outlines the approved methods and techniques for media sanitization!

Benefits of Circular Practice

Carbon Benefits:

Zooming in on the market for hard disk drives (HDD) and solid-state drives (SSD), we can start to look at storage as an overall contributor to carbon emissions and e-waste in the ICT industry. The industry shipped 259 million HDDs in 2021 [1], a number that is declining every year due to the shift of high-capacity nearline drives for hyperscale data centers. The worldwide amount of HDD bytes is expected to continue to grow at 19.1% from 2021 to 2026, reaching over 3 Zettabytes of HDD per year. According to a Seagate conducted LCA, a large capacity HDD contributes 87% of Greenhouse Gas Emissions during the use phase and 45.9kg of CO2e per year.

After interviewing many hyperscalers and ITAD providers, we estimate about 90% of the HDDs today are getting destroyed at the end of first use. HDDs only come in two form factors, so it is easy to estimate the total weight of all the hard drives shipped per year.

Table 1. Hard disk drives (HDD) market size and weight

HDD Type	Average Weight (grams)	2021 Units (millions)	Total Weight
2.5in	200g	96M	19.2M kg
3.5in	670g	162M	108.5M kg

The estimated total weight of shredded metal is 127M kg or 139993.53 tons. The input of such tonnage as “mixed electronics” yields a 110,469 MTCO2e avoided if recycled using EPA’s WARM tool. This, by itself, is not an impressive volume of carbon, about the size of Scope 1 and 2 emissions for a mid-size company, but the commutative impacts year on year are large. What is important is to realize that avoided emissions from the reuse of HDDs are far greater than the raw material, which a typical Life cycle Assessment shows. The actual avoided emissions could be 2.8 M MTCO2e per year, and that is just the HDD, which is not the heaviest metal component of the data center rack.

SSDs ship even more units than HDDs, currently at 429M units per year [2] and the estimated unit count growing 6% between 2021-2026. A Dell server LCA found that 50% of GHG emissions came from the use phase, and the SSDs were by far the largest contributors with most of the contribution coming from the manufacturing of the NAND die. More LCAs of modern SSDs are needed as SSDs have a much greater variety of size, form factor, and capacity. Since most of the carbon from manufacturing SSDs comes from the NAND flash itself, the carbon footprint will scale linearly with SSD capacity, further increasing the importance of reuse as drive capacity grows over time.

Sidebar: OCP Opportunity

The OCP LCA whitepaper details how OCP companies can scope, model, and properly report GHG emissions. Recent OCP storage specifications, like the OCP Datacenter NVMe SSD specification and boot drive specification now require a LCA to be performed by all vendors. This will greatly improve transparency and reporting, making it easier for data center end customers like hyperscalers and OEMs to see the contribution of GHG from storage, and as we will see, the benefit of circular business models.

Solution: Sanitization to unlock circularity for storage

Storing, securing, and processing data in the ICT industry is fundamental to global business. Companies go to great lengths to secure their data and prevent confidential information from being made available to others. When a company is done using its ICT equipment, including the storage device, it is important to render the data inaccessible. At the end of first use, destroying the storage device is common practice to eliminate any perception of risk. Other sanitization methods are available that leave the device in a reusable state, while still eliminating risk of recovering any user data! Unfortunately, many terms are thrown around the industry that do not have a rigorous definition in specifications, like data wiping, data deletion, data destruction, or blindly smashing a device. Fortunately, there is a process called sanitization, with robust specifications on the various techniques.

Sanitization

A process or method to render access to target data on storage media infeasible for a given level of effort.

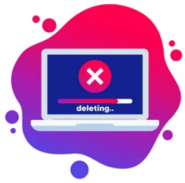
Standards

IEEE P2883 Standard for Sanitizing Storage is the latest international standard that defines sanitization methods and techniques, which is meant to supersede the NIST SP800-88r1.

- Defines Sanitization Methods and Techniques for the specific media type (HDD, SSD, optical, removable, etc.)
- Specifies interface-specific techniques (SATA, SAS, NVMe)
- Align industry on terminology and modern techniques for media sanitization
- Target all logical and physical locations for data – including user data, old data, metadata, overprovisioning, etc.

Sanitization Methods

Figure 1. Sanitization methods defined in IEEE P2883



Clear

Uses logical techniques to remove data on all addressable storage

Prevent against simple non-invasive data recovery

Format, deallocate

Purge

Uses logical or physical techniques to remove all data

Infeasible data recovery with state of the art techniques

Block erase, crypto erase, overwrite

Destruct

Infeasible data recovery with state of the art techniques

Leaves device in unusable state

Disintegrate, incinerate, melt

a. **Clear**: Sanitize using logical techniques on user data on all addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user. E.g. basic file recovery utilities that scan the drive logical blocks for data.

b. **Purge**: This is the most important sanitization method for enabling circularity for storage devices! Purge sanitize uses logical techniques or physical techniques that make the recovery of target data infeasible using state-of-the-art laboratory techniques, but that preserves the storage media and the storage device in a potentially reusable state. Multiple purge methods can be used together to further decrease the probability of recovering data. Still, even a single one of these verified purge techniques is sufficient against state of the art laboratory techniques (disassembly, electron microscopy, x-ray probing, etc.)

   i. **Sanitize Purge Cryptographic erase** (CE) will change the media encryption key on a device, typically today AES256, which is not only a secure way to sanitize a device but also happens in seconds

   ii. **Sanitize Purge Overwrite** securely overwrites the storage media with various patterns that can be verified later. Overwrite can be used with hard drives that don't support CE

   iii. **Sanitize Purge Block Erase** can zero out the erase blocks on NAND based SSDs, and can be used in conjunction with CE

c. **Destruct**: Sanitize using physical techniques that make the recovery of target data infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the storage media for storage. Shredding and pulverizing, which were once approved methods of destruction, are NOT approved sanitization techniques. A small 2mm square shred of a disc platter can contain large amounts of recoverable data. Destruct should only be used if other sanitize methods fail or verification of sanitization fails, for example, if a drive is in a failed state and not responding to host commands.

i. **Melting**: Destruct by changing storage media from a solid to a liquid state, generally by the application of heat

ii. **Incineration:** Destruct by burning a storage device completely

Next steps towards circularity

Use and Reuse

Extending the first use is very important for minimizing the percentage of the LCA carbon and materials impact for the use phase vs everything else (manufacturing, distribution, etc.) HDDs and SSDs generally have a 5 year warranty but are swapped out every 3-5 years. A large data center may do this to increase storage density, meet growing data demands, and improve its TCO. This doesn't mean the TCO of the old drives is not competitive for a large range of uses, either in other organizations at the company or externally! Failure rates increase with use over time, and environmental factors. These drives still have value to other customers, especially for archive, cryptocurrency mining, or lower throughput environments.

Reuse storage with purge media sanitization

Reuse has the largest carbon impact and value recovery for circularity. Purge sanitization is the best for reuse since it prevents data recovery and leaves the device in a usable state. As we learned above, there are multiple methods for purge, which depend on the drive model and firmware for support (Appendix B). Cryptographic erase, which some vendors call Instant Secure Erase (ISE), uses AES-256 data encryption to scramble the data in seconds cryptographically. AES-256 is considered to be quantum compute resistant by the NSA and other governmental agencies and standards groups. For highly sensitive data where a "steal now, de-encrypt decades later" is considered plausible, third-party verified sanitize overwrite technology is an option that takes approximately one hour per terabyte to complete on a modern HDD. Solutions exist for doing this inside a data center or facility in economically viable ways.

OCP Opportunity for Reuse

Adopt IEEE P2883 into the OCP storage specifications. Use an approved purge sanitize technique to safely remove data on a storage device to prepare for the transfer of ownership and reuse. Prioritize device reuse over the destruction to enable the circular economy. Basic verification of sanitization methods are outlined in the specification, but there is an opportunity for OCP members to create standard methods and open-source software for verification of purge. The OCP security workgroup already has a transfer of ownership specification, which can be extended to storage devices with purge sanitization.

Repair

Modern high-capacity hard drives have up to 10 platters and 20 read/write heads. One head failure can impact the ability to read or write to 5% of a drive, but the rest of the drive can continue to operate with high reliability. Drive regeneration technology supported in standards can remanufacture these

drives while preventing data loss and restoring 95% capacity without resorting to removing and destroying the drive. These technologies become more crucial as aerial densities improve with technologies such as Heat Assisted Magnetic Recording (HAMR) and Microwave-Assisted Magnetic Recording (MAMR).

SSDs are made up of dozens to hundreds of NAND dice spread over multiple physical packages. On die XOR or RAID can generally prevent a few die failures on enterprise SSDs today, making them very resilient. SSDs already have a greater maximum capacity than HDDs, with 30TB class drives shipping in volume today. We are not far away from drives that are hundreds of TB. In these types of large drives, they will need more technology to ensure that a small failure does not take down the entire drive (blast radius). Zoned storage (ZNS, or zoned namesapces) in NVMe can achieve similar behavior for fail in place, by taking zones offline in the event of a physical hardware failure like an entire NAND package.

SSDs fail very differently than HDDs, and this is well studied amongst SSD vendors, hyperscalers, and OEMs. SSDs primarily fail because of firmware issues, and a large percentage of the time the underlying hardware is perfectly fine.

OCP Opportunity for Repair

The OCP Datacenter NVMe SSD specification defines two very exciting features, the SMART / Health Information Extended log page (Log Identifier C0h). This allows for fine-grain reporting of SSD stats for AI to do predictive failure analysis on a population of drives. This keeps good drives in service longer while eliminating downtime for failed drives. The Error Recovery log (log page C1h) allows the drive to give hints to the host on what type of failure occurred, and if the drive can be recovered with a low-level format of the media, a hard reset, or other recovery mechanisms. The impact of this is massive, taking the already low failure rate of SSDs (generally lower than 0.44% annual failure rate) down even lower, with the ability to recover from certain firmware failures.

Recycle

If drives must be destroyed, it is best to disassemble and separate the materials prior to shredding the media in order to maximize the recyclability and avoid downcycling. Most recycling methods today shred the entire drive, which mixes all the materials together, and focus on recovering aluminum which is only a small fraction of the recycling potential in terms of value and environmental impact. The most critical resource to recover is the rare earth neodymium magnet. Value recovery of recycling components on hard drives has been well studied [5] and drive reuse has by far the largest impact on GHG compared to recycling magnet assemblies, magnets, or raw materials.

Table 2. Impact per lifecycle of various processes

Process	Impact per lifecycle
Reuse drive	5.5 kg CO2e
Reuse magnet assembly	1.9 kg CO2e
Magnet to Magnet recycling	0.7 kg CO2e

Hydrometallurgical	-0.3 kg CO2e
Recycle for material	0.02 kg CO2e

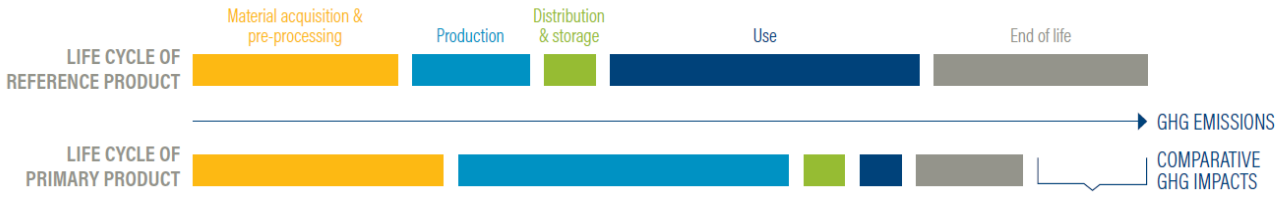
Description: Life cycle assessment of emerging technologies on value recovery from hard disk drives

GHG Accounting for Circular Business Models

Accounting the GHG impact for reuse can be incredibly challenging. Some storage vendors have been providing LCAs for recent products, which is ahead of other ICT components. Others have only provided LCAs to their customers for system-level LCAs, and currently, it is difficult to find product-specific LCAs for SSDs on the top vendor websites. Methods exist to estimate comparative products, or products that have effectively the same use. This can be incredibly challenging for the ICT industry where products come in various SKUs, form factors, and packaging.

> **Comparative impact**: The net difference in GHG emissions and removals between a base case without the assessed product and the case with the assessed product.
>
> Comparative impacts are estimated as the difference between the total, attributional, life-cycle GHG inventories of a company's product (the "assessed" product) and an alternative (or "reference") product that provides an equivalent function. [6]

Figure 2. Calculating Comparative GHG Impacts Using the Attributional LCA Approach



A comparative impact analysis may be useful to compare the LCA of a first use and second use of the same device, which will show the delta in manufacturing GHG, EOL, and others. It may also be useful for comparing multiple second use devices vs a single first use device, if storage vendors want to normalize on performance or capacity (per terabyte). It is important to note that a comparative assessment does not take precedence over companies correctly reporting scope 1, 2, and 3 emissions, which requires accurate product LCAs.

A consequential model can estimate the change in emissions or removals caused by a specific decision or action. We suggest companies explore these models for drive reuse.

> **Consequential approach**: A method that estimates comparative GHG impacts as the total, system-wide change in emissions and removals that results from a given decision or intervention. [6]

The consequential approach may be useful for deciding to extend the life of a storage device, or the impact of giving the device a second use instead of physical destruction.

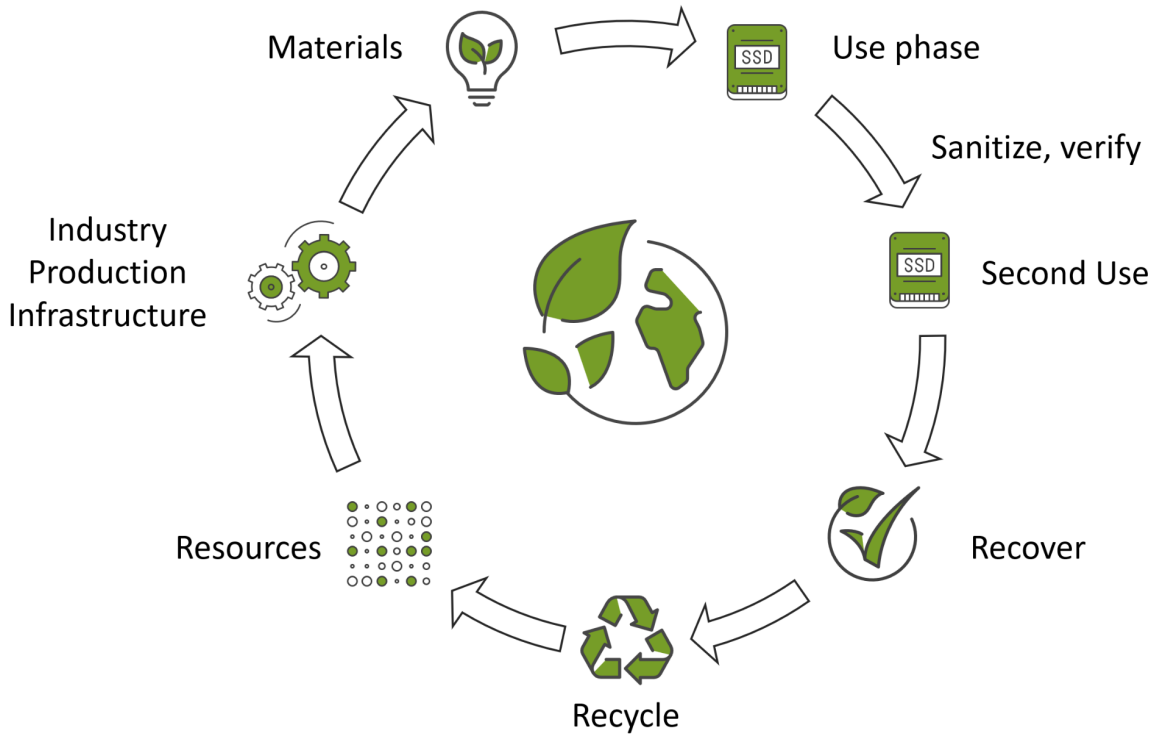
The Ellen MacArthur Foundation has developed the Material Circularity Indicator (MCI), which is a strong foundation; however,moving forward it can be improved to better support the ICT industry. You can see an example LCA that contains an MCI from a Seagate HDD. One vendor suggested doing a separate LCA for each use, which would lend itself to comparing the manufacturing carbon easily.

The impact for extending the use can be in a reduction in a company's scope 3 emissions. The company can also reduce the impact of the EOL phase in an LCA if the device gets reused. Since a large percentage of the carbon in an SSD LCA comes from pre-use (manufacturing, specifically the NAND flash) extended use will offer a large reduction by amortizing that carbon over a larger period of time. A longer first use also means that companies will have to purchase less equipment, reducing the scope 3 emissions for purchased goods and services.

Not enough of the current circularity metrics prioritize device reuse over material reuse and recycling, despite the clear data showing that it is the highest value recovery and materials flow for a circular business model.

Conclusion - Call to Action

Figure 3. Example circular economy for a storage device



Description: The circular economy enables materials to go through the highest value flow possible

Privacy is not only a fundamental human right but essential to enterprise needs. The shift to cloud computing has made companies' workloads and data more agile, scalable, and cost-effective. This required a tremendous amount of trust from the cloud service providers and did not happen overnight. These CSPs promise trust in the technology, operations, policies, and industry collaboration. Technology has delivered strong encryption protocols that protect user content by securing data at rest and in flight. Data at rest security uses encryption, e.g. self-encrypting drive or Microsoft BitLocker, to protect against the very unlikely scenario of someone obtaining physical access to a device. Data in-flight security is done to prevent unauthorized parties from eavesdropping with internet technologies like TLS. With the massive growth of cloud computing and storage, it is safe to say that there is already a considerable amount of trust in today's security and encryption technologies. So why does this suddenly break down when a device is leaving organizational control? When a device is at the end of its first use?

Hyperscalers have made public commitments to circularity by making goals of 90% reuse by 2025. Reuse goals need to prioritize actual device reuse as the most significant impact on circularity rather than recycling. Reusing raw materials is a step towards circularity, but the value recovery and carbon impact from giving the drive a second and/or third has been proven to be vastly more impactful, up to 275x. [5]. These public commitments can't somehow exclude storage devices because it is hard or

because they store data. Safe media sanitization with a purge can ensure data does not get into the wrong hands while enabling the circular economy for storage.

While security experts are constantly improving encryption and forward-thinking, AES 256 is considered safe today. Companies have independently verified their purge techniques cannot be recovered, even with expensive and time-consuming forensic analysis. Verification, automation, and sanitization at scale is a great opportunity for the ITAD companies that used to rely on physical destruction business models.

More from OCP is coming with the new Design for Circularity guide, but a few ideas for making storage more circular is:

- Promote and support security features to enable purge sanitization
- Include robust drive health, monitoring, and recovery features to keep drives running as long as possible
- Make drives with easy disassembly for recycling when device fails
- Use recycled material wherever possible

In this decade of climate action, as companies set increasingly aggressive carbon reduction goals and timelines, the transitioning from wasteful linear models to regenerative ones is gaining momentum. This shift away from take/make/waste in favor of reuse/repair/refurbish/remanufacture has been growing, as early adopters share stories of their financial and environmental gains.

About Open Compute Foundation

The Open Compute Project Foundation is a 501(c)(6) organization which was founded in 2011 by Facebook, Intel, and Rackspace. Our mission is to apply the benefits of open source to hardware and rapidly increase the pace of innovation in, near and around the data center and beyond. The Open Compute Project (OCP) is a collaborative community focused on redesigning hardware technology to efficiently support the growing demands on compute infrastructure. For more information about OCP, please visit us at http://www.opencompute.org.

About Circular Drive Initiative

The Circular Drive Initiative (CDI) is a collaboration of global leaders in digital storage, data centers, sustainability, and blockchain in a joint effort to reduce e-waste by promoting and enabling the secure reuse of storage hardware. CDI was convened under the leadership of William McDonough, Chief Executive of McDonough Innovation and the renowned architect of Cradle to Cradle design and The Circular Economy, which brings circular design principles and reporting to data storage in the ICT industry. CDI is tackling the barriers of data security, regulations, market enabling, metrics, and operations to facilitate the reuse of storage devices and reduce GHG emissions and e-waste. Visit us at https://circulardrives.org

References

1. IDC Worldwide Hard Disk Drive Forecast, 2022–2026. May 2022 - Market Forecast - Doc # US49050622
2. Worldwide Solid State Storage Forecast, 2022–2026, May 2022 - Market Forecast - Doc # US47831722
3. IT Renew LCA model case study
4. Kali Frost, Ines Sousa, Joanne Larson, Hongyue Jin, Inez Hua, Environmental impacts of a circular recovery process for hard disk drive rare earth magnets, Resources, Conservation and Recycling, Volume 173, 2021, 105694,ISSN 0921-3449,
5. Hongyue Jin, Kali Frost, Ines Sousa, Hamid Ghaderi, Alex Bevan, Miha Zakotnik, Carol Handwerker, Life cycle assessment of emerging technologies on value recovery from hard disk drives, Resources, Conservation and Recycling, Volume 157, 2020, 104781, ISSN 0921-3449
6. Russell, Stephen. 2018. “Estimating and Reporting the Comparative Emissions Impacts of Products.” Working Paper. Washington, DC: World Resources Institute. Available online at https://www.wri.org/research/estimating-and-reporting-comparative-emissions-impacts-products

License

OCP encourages participants to share their proposals, specifications and designs with the community. This is to promote openness and encourage continuous and open feedback. It is important to remember that by providing feedback for any such documents, whether in written or verbal form, that the contributor or the contributor's organization grants OCP and its members irrevocable right to use this feedback for any purpose without any further obligation.

It is acknowledged that any such documentation and any ancillary materials that are provided to OCP in connection with this document, including without limitation any white papers, articles, photographs, studies, diagrams, contact information (together, “Materials”) are made available under the Creative Commons Attribution-ShareAlike 4.0 International License found here: https://creativecommons.org/licenses/by-sa/4.0/, or any later version, and without limiting the foregoing, OCP may make the Materials available under such terms.

As a contributor to this document, all members represent that they have the authority to grant the rights and licenses herein. They further represent and warrant that the Materials do not and will not violate the copyrights or misappropriate the trade secret rights of any third party, including without limitation rights in intellectual property. The contributor(s) also represent that, to the extent the Materials include materials protected by copyright or trade secret rights that are owned or created by any third-party, they have obtained permission for its use consistent with the foregoing. They will provide OCP evidence of such permission upon OCP’s request. This document and any "Materials" are published on the respective project's wiki page and are open to the public in accordance with OCP's Bylaws and IP Policy. This can be found at http://www.opencompute.org/participate/legal-documents/. If you have any questions please contact OCP.

Appendix A: Industry Standards

IEEE P2883: "IEEE Approved Draft Standard for Sanitizing Storage," in IEEE P2883/D18, April 2022 , vol., no., pp.1-69, 21 June 2022.
This is the latest and most comprehensive industry standard for storage sanitization, encompassing and superseding NIST SP800-88, ISO/IEC 27040 and other standards. IEEE P2883 has a strong focus on circularity. The scope of IEEE P2883 covers all physical and logical locations that currently contain user data, used to contain user data (e.g., deallocated data, data reallocated because of media errors),could contain user data (e.g., overprovisioning, unused capacity, spare pools),are able to contain data that discloses information about user data (e.g., data that is usable to direct forensic analysis.

NIST SP800-88R1: This document from the National Institute of Standards and Technology (NIST) contains guidelines for media sanitization and storage security, but does not define requirements. It is a product of the US government and commonly referenced by the NSA, other standards and US companies, but many countries will not refer to US security standards.

ISO/IEC 27040:2015: Information technology – Security techniques – Storage security. Provides general guidance for storage security. It includes no requirements, only recommendations and contains media-specific and interface-specific guidance for sanitization techniques. Contains much common text with NIST SP800-88r1. Edition 2 is under development.

ErP lot 9 was founded in 2019 out of EU ErP (Ecodesign in Europe) Regulations for Storage Products. It defines environmental engineering (EE) and energy efficiency measurement methodology and metrics for servers . ETSI EN 303 470 V1.1.0 (2019-01). Its focus is on power efficiency not data sanitization.

Appendix B: Storage security features

Drive types

For either HDDs or SSDs, there are different categories of security offerings. All offer industry-standard sanitization methods compliant with the "Purge" functionality, whether these drives are SATA, SAS, or NVMe devices. The types primarily are distinguished by their levels of encryption and access control:

Self-encrypting drive (SED): This may be terminology to describe a drive that transparently encrypts all on-disk data. OEMs may use this term exclusively to describe a drive that supports TCG specifications, like Opal. Features like ISE may only be available for a sku that is designated as a SED drive. Most SSDs contain a media encryption key and scrambler on the SSD controller independent of host user key and passwords. SED may be used to describe a drive with both encryption capabilities and access control (e.g. password).

Secure Erase (SE): SE drives may be sold without encryption enabled, meaning that the data on the media is stored in the clear. Sanitization is performed by *overwriting* the data and reserved areas of the disk (for HDD) or by performing *block erase* commands on the data and reserved areas of the NAND (for SSD). The operations are not instantaneous, and in the case of HDDs, can take many hours to perform.

Instant Secure Erase (ISE): ISE drives pass all data through the drive's encryption engine, so that the data is encrypted at rest on the media, whether disk or NAND. ISE drives support *cryptographic erase*, where the drive is erased by destroying the encryption key for the data on media, rendering it unreadable. Because this key can be destroyed effectively instantaneously, these drives can be erased instantly as well.

Trusted Computing Group (TCG): TCG drives pass all data through the drive's encryption engine, and the data will thus be encrypted at rest on media. TCG drives can utilize the same *cryptographic erase* methodology to instantly render the drive unreadable. TCG drives can also support *Revert* commands which can be used to reset the drives cryptographic authentication settings, or all of the drive's settings, to factory default. TCG drives are available supporting TCG Enterprise, TCG Opal, and TCG Ruby authentication protocols, but for the purposes of sanitization, these are all equivalent and support cryptographic erase.

FIPS (TCG-FIPS): TCG-FIPS drives are functionally identical to TCG drives, and support *cryptographic erase*. The differentiator between these drives and TCG drives is that the encryption and authentication must be certified by an NIST-approved lab as Federal Information Processing Standards (FIPS) 140-2 or 140-3 compliant.

For the purposes of sanitization in a circular economy, ISE, TCG, and TCG-FIPS drives all provide instant sanitization capability using *cryptographic erasure* consistent with the NIST 800-88 or IEEE P2883 "Purge" functionality. Due to import/export restrictions, however, many drives sold into the market are of the Secure Erase type. These drives can also be sanitized consistent with the NIST and

IEEE “Purge” functionality, but this must be done with the *overwrite* or *block erase* methods, which are not instantaneous.

Appendix C – ICT Server Component Basics

Items	Description
Chassis	A server chassis is a metal structure that is used to house or physically assemble servers in various form factors.
PSU	PSU stands for power supply unit, an internal IT hardware component. Instead of supplying the systems with power, it converts the electricity source into the correct voltage. By receiving power from an electrical outlet, it converts the current from AC (alternating current) to DC (direct current).
NIC + FPGA	A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing – hence the term field-programmable.
GPU	A graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device. These units form the backbone of most artificial intelligence and gaming workloads.
CPU	The central processing unit (CPU) is a hardware component found in the circuit board of your computer or smart device. It looks like a tiny silicon chip, but it has enormous computing power thanks to its built-in transistors.
HDD	A hard disk drive is a mechanical device used to store data, containing disk platters, a motor, and read/write heads to magnetically record data. HDDs for data centers are typically in the 3.5in form factor, and use the SATA or SAS interfaces.

SSD	A solid-state drive (SSD) is a data storage device that uses non-volatile memory to store persistent data, most often NAND flash memory. SSDs have no moving parts and are known to be reliable, low power, low latency, and high performance.
Motherboard	A motherboard is a printed circuit board containing the principal components of a computer or other device, with connectors into which other circuit boards can be slotted.
NVDIMM	An NVDIMM (non-volatile dual in-line memory module) is hybrid computer memory that retains data during a service outage. NVDIMMs integrate non-volatile NAND flash memory with dynamic random access memory (DRAM) and dedicated backup power on a single memory subsystem.
Memory (Server RAM)	Server memory is Random Access Memory (RAM) which processes data from HDDs to the CPU. As a form of volatile memory, when server memory is powered off it loses all its held information.
Rack	A rack is a standardized frame or enclosure for mounting multiple electronic equipment modules.
Cables	Electrical cables are used to connect two or more devices, enabling the transfer of electrical signals or power from one device to the other. Effective rack cable management helps to improve physical appearance, cable traceability, airflow, cooling efficiency, troubleshooting time as well as elimination.
Fans	Fan trays are used to help move heat out of a rack and are mounted wherever a hot spot might exist. For instance, if there is no equipment at the top of an enclosed rack, that area can become hot due to low circulation.
PDU	A Power Distribution Unit (PDU) is a device with multiple outlets designed to distribute power to computers, servers, network switches and other IT devices in a rack. PDUs come in a variety of styles that provide everything from basic power distribution to enhanced remote power management.

Network Device	Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network. Here is the common network device list: Hub, Switch, Router, Bridge, Gateway, Modem, Repeater, Access Point