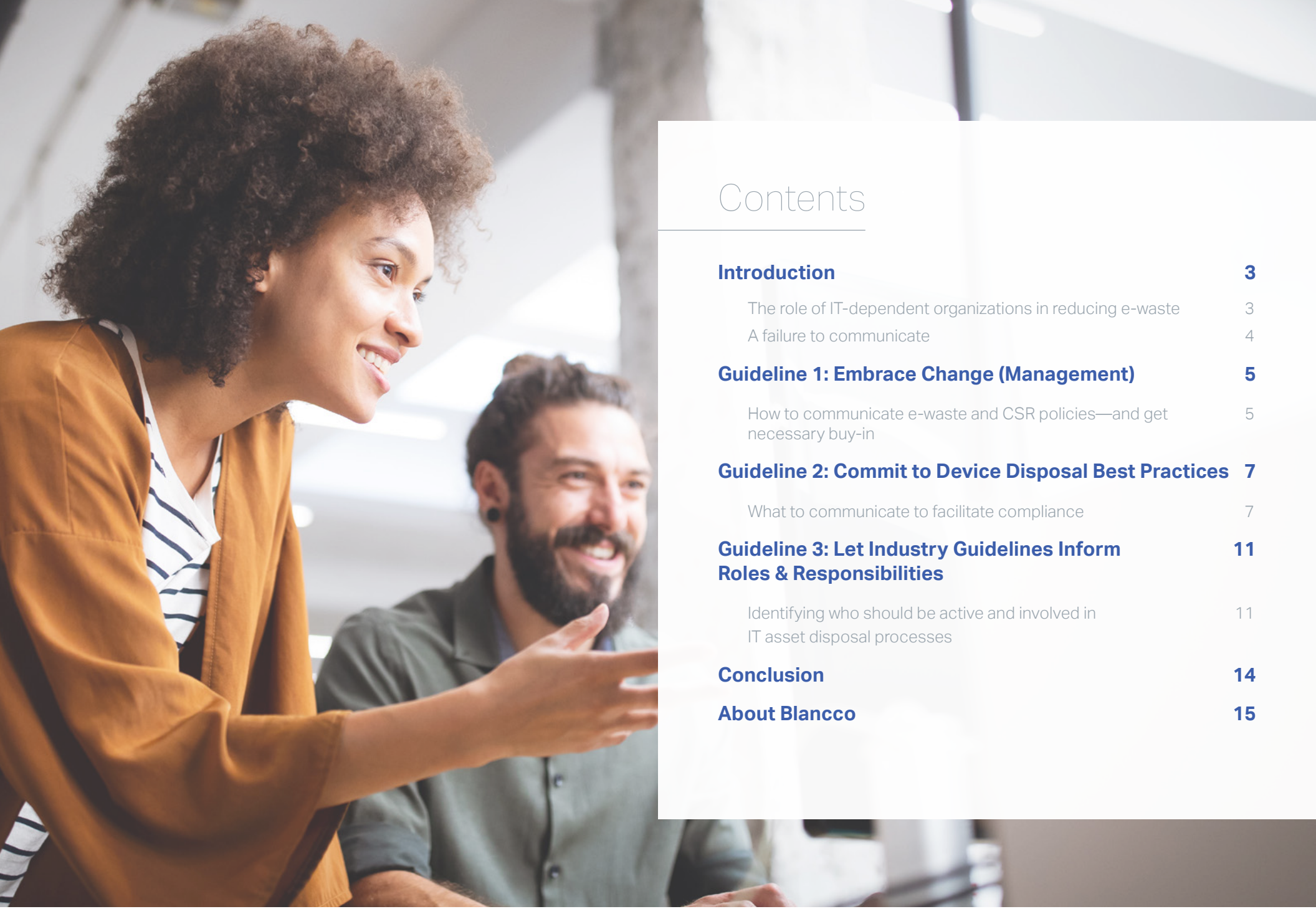
EBOOK

3 Guidelines for Communicating *(and Implementing)* Eco-Friendly IT Asset Disposal Policies

December 2020

blancco



Contents

The role of IT-dependent organizations in reducing e-waste

Globally, companies are realizing the value of being about more than just profit. Community investment, generous employee programs, support of humanitarian causes and volunteerism are just a few ways enterprises have incorporated corporate social responsibility (CSR) within their business goals and policies. In doing so, these organizations cultivate public goodwill, boost internal morale and advance corporate values.

Such policies can also be financially fruitful. Customers and job seekers now prioritize "giving back" as a natural response to business growth, often choosing to do business with companies that reflect their ideals. Investors also look at companies' environmental, social and governance (ESG) policies as a means of evaluating risk and longevity.

In this climate, IT-dependent organizations have a great opportunity to create positive change when disposing of their data storage hardware, including servers, PCs, laptops, drives and phones.

According to the *Global E-waste Monitor 2020 (PDF)*, more than 53 million metric tons of electronic waste, or e-waste, was produced in 2019 alone. Monitors, laptops, notebooks, tablets, personal computers, printers, routers and mobile phones make up about 20 percent of this amount, though some reports indicate up to nearly half.[1] It's unsurprising, therefore, that processes regarding enterprise technology use and disposal can play a key role in reducing the amount of digital technology that finds its way into landfills.

The challenge, however, is that while many organizations have CSR or e-waste policies in place to minimize needless technology disposal, these policies fail to be fully communicated throughout the organization. In other words, intentions are good, but execution falls short.

The good news is, this can change.

[1] Global E-Waste Monitor 2020 reports that of the approximately 53.6 million metric tons (Mt) of e-waste generated, the Screens and Monitors category, which includes televisions, monitors, laptops, notebooks and tablets weighted 6.7 Mt, while the Small IT and Telecommunications equipment category, which includes routers, personal computers, printers and telephones, weighed 4.7 Mt. This does not include copying equipment and potentially other digital devices. The January 2019 report, *A New Circular Vision for Electronics* from the World Electronic Forum states that "one-half of all e-waste is personal devices, such as computers, screens, smartphones, tablets and TVs."

A failure to communicate

In 2020, Blancco commissioned Coleman Parkes Research to survey 600 global enterprise leaders on their IT asset disposition policies. Findings were recorded in the 2020 research report, *The Rising Tide of E-Waste: How Environmental Concerns and Shifting Work Patterns are Shaping Device Management Practices*.

Various IT asset disposition options, including opportunities for device recycling and reuse, can all be specified in an e-waste policy. Yet merely having a policy isn't enough: The study found that while 94 percent of organizations surveyed had an e-waste policy defined, *only half had a dedicated e-waste policy in place that was communicated across the whole organization*.

Digging deeper, the data revealed several reasons for this lack of effective policy communication. Three primary ones were:

- Uncertainty on how best to communicate these important initiatives (47 percent for e-waste and 56 percent for CSR policies)
- A lack of clarity around the policies themselves (46 percent for e-waste and 42 percent for CSR policies)
- Unclear ownership of e-waste and CSR policies (39 percent for e-waste and 45 percent for CSR policies)

The lack of clear ownership for communicating and executing on these policies hinders an enterprise's ability to mitigate environmental, reputational and data security risks. To move from policy to practice, enterprise leaders can overcome these challenges by looking to

- **Change management principles** – for **HOW** to communicate a new or revised policy and get buy-in
- **Device disposal best practices** – for knowing **WHAT** to communicate to ensure data security and audit-ready compliance with data protection requirements
- **Industry guidelines and project management tools** – for understanding **WHOM** to involve and at what level

While each enterprise differs in organizational structure, the following three guidelines will assist organizations in both communicating and carrying out their e-waste and CSR policies successfully.

Guideline 1: Embrace Change (Management)

How to communicate e-waste and CSR policies—and get necessary buy-in

> Many companies care about corporate social responsibility (CSR). But putting it into practice requires more than CEO speeches and company policies; managers and employees have to be on board, so that initiatives can be implemented and momentum for CSR can be sustained."

Harvard Business Review, "How CSR Managers Can Inspire Other Leaders to Act on Sustainability" hbr.org

In our survey, uncertainty on how best to communicate e-waste and CSR initiatives was the primary challenge to "spreading the word" within the organization. To address this, enterprises can lean on the discipline of *change management*.

The Association of Change Management Professionals (ACMP) defines change management as "the practice of applying a structured approach to transition an organization from a current state to a future state to achieve expected benefits." Within this discipline, there is *change management communication*.

In most enterprises, technology use spans departments and various levels of technical expertise. And, because e-waste policies (or CSR policies with e-waste components) deal with disposal of data storage devices, such policies also affect data security. It is therefore to the organization's benefit to reach each staff member appropriately and have everyone informed and supportive of e-waste and IT asset disposal policy changes.

To encourage buy-in:

- **Communicate broadly.**
  Ideally, even before a policy is formed, a cross-disciplinary group will have weighed in on risks, benefits, expected outcomes and implementation. Once the policy is adopted, change management leaders advise communicating the policy through the most executive policy sponsor and each staff member's immediate supervisor.[2] Standard communication channels—company and team meetings, newsletters, executive communications, training sessions, for example—can also help disseminate appropriate details about the policy and related processes. Consider supplemental communications unique to the rollout, such as special announcements, activities and scheduled reminders. Group members who worked on formulating the policy can further communicate by being ambassadors within their respective realms of influence.

- **Communicate the "why."**
  Be clear about the reasons behind the policy change. Does it align with company values? Are there new regulations in place? Is there a risk that is being addressed? Help teams at all levels understand the environmental, data privacy and regulatory reasons behind the policy implementation. Adjust communications based on role or use.

[2] Prosci, "10-Question Checklist on Change Management Communication." Accessed December 4, 2020 from *www.prosci.com/resources/articles/change-management-communication-checklist*.

Communicate the benefit.
Different benefits will resonate more strongly with different audiences and will help offset any additional effort or resources required to implement the policy. Does the policy lower data breach risk? Conserve environmental resources? Provide greater data privacy protection for job applicants or financial records? Boost brand and investment appeal? Stress these benefits in appropriate detail for each role. Otherwise, you could miss a chance to match employee desires with what the enterprise needs to accomplish.[3]

Communicate needs and expectations.
As with cybersecurity, e-waste handling extends beyond the technology team. Budget requests will need to be approved, operational staff will need to know timelines and procedures, all staff will need to know why used removable media (for example) shouldn't simply be thrown away. Measures should also be put in place to verify that enterprise policy requirements are being met by each staff member as appropriate. Celebrate successes (e.g., the percentage of e-waste diverted from physical destruction each year) and require change when policies are neglected or misapplied. If a lack of implementation is widespread, evaluate how and what is being communicated.

Whether e-waste policies are initiated by the C-suite, IT department or concerned staff, it is critical that anyone affected by the policy be knowledgeable, and ideally, persuaded, not only about what processes the policy will change, but why, how it benefits them individually and what will be needed or expected from them in order for policy implementation to be successful.

[3] Prosci, "10-Question Checklist on Change Management Communication." Accessed December 4, 2020 from *www.prosci.com/resources/articles/change-management-communication-checklist*.

Guideline 2: Commit to Device Disposal Best Practices

What to communicate to facilitate compliance

In *The Rising Tide of E-Waste*, respondents noted a lack of clarity around e-waste and CSR policies as a leading factor hampering policy communication within the organization.

According to the *Global E-Waste Monitor 2020*, only 17.4 percent of the 53.6 million metric tons of e-waste produced in 2019 was properly collected and recycled. Unfortunately, a great deal of enterprise e-waste is discarded improperly, putting both the environment and sensitive data at risk.

Our 2019 research study, *A False Sense of Security*, revealed that a third of the world's largest enterprises use inadequate data sanitization, such as formatting, freeware-based overwriting or physical destruction without an audit trail, to prevent data breaches at end-of-life. Such inadequate practices can leave sensitive data behind. They can also fail to prove to regulators that the enterprise is following data protection requirements.

Furthermore, physical destruction of perfectly usable data storage devices deprives organizations from getting full value from their IT investment, contributing needlessly to landfills and potentially toxic disposal.

Whether an e-waste policy benefits or harms an organization will depend on the processes specified within the policy. To benefit the environment without leaving data behind, an e-waste policy should include (or refer to procedural documents that include):

- **Device collection processes and procedures.** It is critical that all teams understand how and when used devices are to change hands. To protect against data loss, assets should not be allowed to leave their original working premises with data remaining on them. In an era of remote work, centrally managed remote erasure by an IT asset disposition vendor or the enterprise itself can address devices used both inside and outside the office environment. Similar processes can also be used to sanitize data from servers or storage systems in various data center locations. Whenever possible, these sanitization processes should be immediate, automated, zero-touch and fully auditable, and these concepts should be specified throughout related documentation.

- **Data sanitization methods to be used for various types of media, data sensitivity and asset condition.** This guidance can be based on regional or global standards, such as NIST 800-88 from the U.S. National Institute of Standards and Technology, the U.K. National Cyber Security Centre's guidelines on data disposal or other data protection guidelines. Proper sanitization includes verification of the destruction and a certificate of erasure for audit purposes. If a device is no longer functional, a certificate of physical destruction to the right standards and requirements should be issued. For functional devices, certified software-based data-erasure enables enterprises to confidently redeploy devices internally, send back after lease, send back to an OEM or sell, donate or use them for spare parts.

- **Data sanitization timeframes.** Immediate data sanitization offers the most data protection for decommissioned assets, as storing or transporting used devices for any length of time leaves data vulnerable to loss, theft or other unauthorized access. Automated erasure at the time of removal from operations eliminates this risk efficiently and should be the aim for best practices implementation.

- **Chain of custody processes.** Keeping track of each asset as it moves along the disposal process assures the organization that all data and data-bearing devices are accounted for. Measures should be in place for both internal and outsourced (i.e., through an IT asset disposition vendor (ITAD) or recycler) collection, sanitization and disposal processes. This is especially crucial when immediate sanitization over the network has not been a viable option during the decommissioning process.

- **Audit-ready documentation.** To prove compliance with regional and industry regulations, e-waste disposal policies must require proof of secure data destruction before assets are reused, sold, donated or recycled. Third-party disposition providers and internal asset management teams should both be able to track each device and provide this documentation.

If policy specifics are muddy, data-bearing devices could be mishandled or misplaced, increasing the risk that a well-intentioned e-waste policy simply exposes the organization to a data breach.

That brings us to clarifying responsibilities.

Case Study: Ayala

Ayala Corporation is one of the largest conglomerates in the Philippines with businesses in real estate, financial services, telecommunications and a broad range of investments. The company also has a deep commitment to corporate social responsibility and supporting the welfare of the surrounding community. One way Ayala Corporation expresses this commitment is by contributing previously owned but highly operational IT hardware so other organizations can use them.

Read the **case study**.

Guideline 3: Let Industry Guidelines Inform Roles & Responsibilities

Identifying who should be active and involved in IT asset disposal processes

> "Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the program and for ensuring program success. Senior management is responsible for ensuring that the resources are allocated to correctly identify types and locations of information and to ensure that resources are allocated to properly sanitize the information."

NIST S.P. 800-88, Rev 1, "Guidelines for Media Sanitization"

The U.S. *NIST S.P. 800-88, Rev. 1, "Guidelines for Media Sanitization*," is a globally referenced document that specifies data destruction methods for IT assets. Renowned for its sanitization categories of Clear, Purge and Destroy, it also includes a "Roles and Responsibilities" section. While targeted to U.S. federal agencies, it's likely to be helpful to private enterprises and non-U.S. organizations.

In the *Rising Tide of E-Waste* research study, the roles respondents cited as being best suited to **implement** an e-waste policy were Head of IT Operations (18 percent), Data Protection Officer (17 percent) and Chief Information Security Officer (16 percent).

But when it comes to ensuring **compliance** with the policy, respondents ranked Head of Compliance first (36 percent), followed by Legal (22 percent) and then Chief Information Security Officer (11 percent).

Actual responsibility for implementation and enforcement will differ according to company size, reporting structures and job titles, but a few of the NIST roles and recommended division of labor are summarized below. Private sector equivalent titles are noted in brackets ():

- **Program Managers/Agency Heads (C-suite, Upper Management):** Responsible for resource allocation and program support.
- **Chief Information Officer (CIO or Chief Information Security Officer):** Puts policy into effect and acts as information custodian; ensures sanitization requirements follow NIST guidelines.
- **Information System Owner:** Ensures contractual agreements protect the confidentiality of system media and that protections are commensurate with impact of disclosure.
- **Information Owner/Steward:** Ensures supervision of onsite media maintenance by service providers, that service providers understand information sensitivity and that users grasp information confidentiality and basic requirements of data sanitization.
- **Property Management Officer (IT Asset Manager):** Ensures that sanitized media and devices that are redistributed within the organization, donated or destroyed are properly accounted for.
- **Records Management Officer (Data Retention Officer):** Advises on data retention requirements so records are preserved appropriately.
- **Privacy Officer:** Advises on privacy issues surrounding the disposition of privacy information and the media upon which it is recorded.
- **Users:** Responsible for knowing and understanding the confidentiality of the information they are using to accomplish their assigned work and ensure proper handling of information.

A note on Data Protection Officers: The EU's General Data Protection Regulation established the role of DPO to protect EU data subjects. According to the UK's Information Commissioner's Office, *"DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations...,"* among other tasks.

To further clarify who does what regarding an enterprise e-waste policy, it may be helpful to formally document and communicate responsibilities via a "RACI matrix." This type of responsibility chart, often used in project management, describes how different roles relate to tasks, decisions or deliverables for a project or business process.

The letters in **RACI** stand for:

- **Responsible** – those who do the work, make the decision or fulfill the task.
- **Accountable** – those who must sign off on or approve the work, task or decision.
- **Consulted** – those who need to provide input before the work can be done or approved.
- **Informed** – those who may need to be updated on progress or decisions.

Getting consensus on how tasks are distributed and making a RACI chart (or other *responsibility distribution model*) part of enterprise policy can help streamline e-waste implementation, ensure responsibility and accountability, help teams monitor and respond to compliance issues and provide clarity throughout the organization. As with all other policy content, this can be updated as needed.

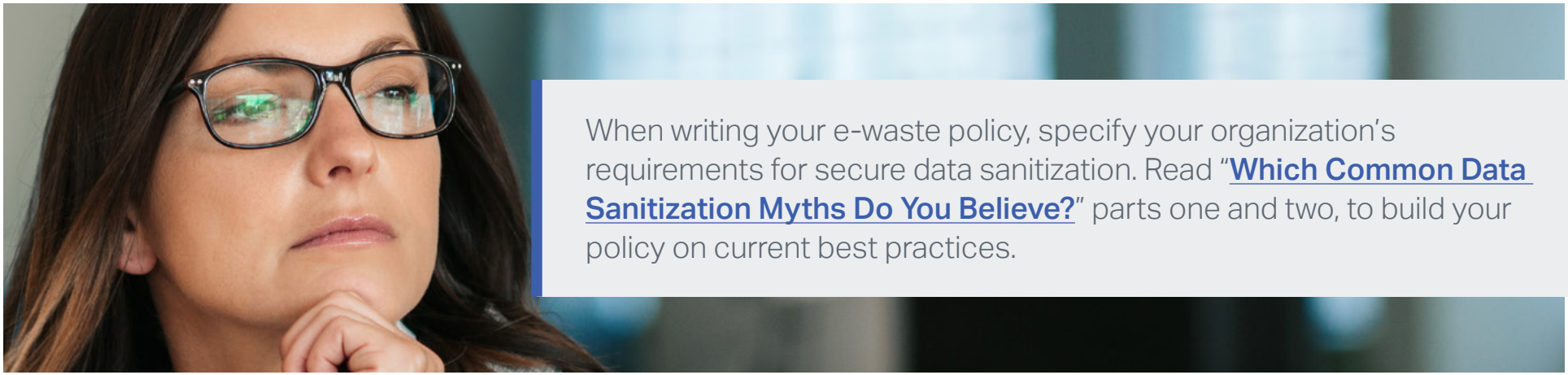
Conclusion

Data protection is starting to become a "social good" in its own right as global regulations tighten data protection requirements on behalf of consumers. And organizations that prioritize secure disposal at device end-of-life are already demonstrating a commitment to meeting social and market demands for safeguarding sensitive data.

Those who have CSR and e-waste policies in place also indicate an awareness of the need to **take care of natural resources** even as technology use continues to grow.

But both are needed. Otherwise, enterprises not only run the risk of contributing to air, water or soil pollution, particularly in the world's poorest countries, but also experiencing a data breach if IT assets are improperly disposed of.

CSR and e-waste policies that encourage device reuse or recycling must do so with data protection in mind. Keeping individual benefits and company purpose front and center of policy communications will help employees understand the reasons for policy changes—and their role in both data protection and environmental stewardship. By drawing from other disciplines, IT-driven organizations can ensure that effective communication happens throughout the organization, that roles and responsibilities are clearly defined to ease implementation—and that policies are set up for success.



When writing your e-waste policy, specify your organization's requirements for secure data sanitization. Read "**Which Common Data Sanitization Myths Do You Believe?**" parts one and two, to build your policy on current best practices.

About Us

Blancco is the industry standard in data erasure and mobile device diagnostics software. Our data erasure software provides thousands of organizations the tools they need to enable sustainable data sanitization processes across the widest array of IT assets. By focusing on erasing and reusing assets instead of physically destroying them, organizations can improve their security posture and address corporate social responsibility requirements, while also ensuring compliance with local and global data privacy requirements.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories. All Blancco erasures are verified and certified, resulting in a tamper-proof audit trail.

With Blancco Mobile Solutions, organizations can achieve real-time valuation for mobile devices with a simple tool that enables consistent, accurate and measurable diagnostic testing, in-store or remotely via a customer-facing app, with workflows purpose-built for buy-back/trade-in, mobile insurance and returns reduction.

Additionally, mobile processors can achieve operational excellence while maximizing profits with Blancco Mobile Diagnostics & Erasure—a purpose-built solution that streamlines diagnostics, erasure and grading processes to prevent unnecessary touchpoints and increase efficiency.

For more information, contact your Blancco provider today.