IRON MOUNTAIN®

PUBLIC SECTOR SOLUTIONS

WHITE PAPER

IT ASSET DISPOSITION THE RIGHT WAY: PREVENT A DATA BREACH

CONTENTS

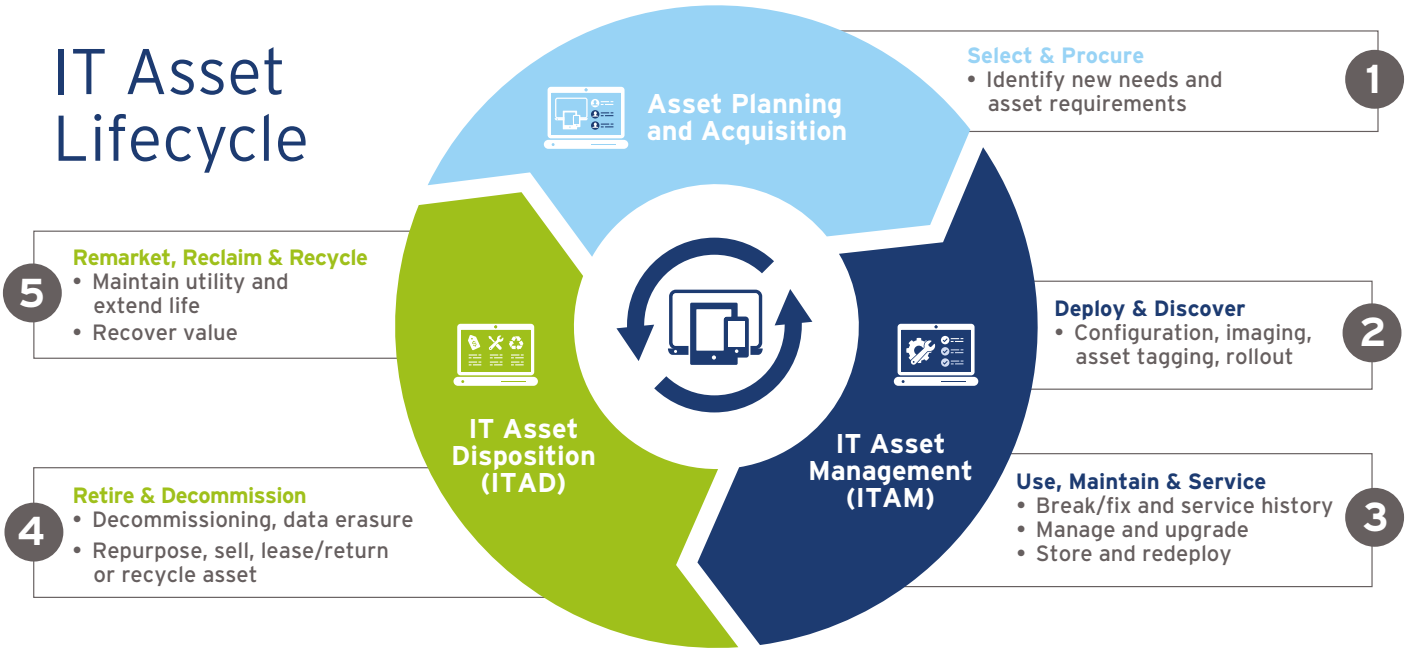
GROWTH IN ELECTRONIC DATA AND TECHNOLOGY MODERNIZATION

The technology that creates, enables, and communicates the growth in electronic data, continues to proliferate at an exponential pace. In order to evolve with this growth, while working to achieve their missions, government agencies are following trends and adopting new technologies, especially those that are data-bearing assets - laptops, PCs, servers, printers and mobile devices.

As devices become outdated or reach the end of their useful life, agencies need to ensure that each individual asset is taken care of in a secure and sustainable way.

Given the security, privacy, and environmental concerns associated with the retiring of IT assets, agencies must ensure they are taken care of in a responsible manner and in adherence to government regulations. A comprehensive IT Asset Disposition (ITAD) program needs to be part of every agency's overall data management strategy.

Disposing of obsolete assets in a manner that is legal, safe, cost-effective, and free of institutional harm is a challenge for all government agencies. Achieving ITAD success requires navigating legal and regulatory requirements, including NIST 800-88 standards, PIPEDA, the proposed Digital Charter Implementation Act 2022, and other provincial privacy requlations (e.g. Quebec's Bill 64). Poorly executed disposition of IT assets can result in fines, public health and safety issues, breaches in data security, and reputational harm.



It's estimated that nearly 80% of the Government of Canada's roughly 8,000 IT services are housed in aging data centres. Most agencies do not have a solid understanding about what data they have or where it is located. While most Canadians have faith in organizations to safeguard their information, two in five (38%) are not confident that their personal information can be kept safe, with 17% saying they are "pretty cynical" about the ability of companies or governments to protect their data. (KPMG in Canada cybersecurity poll, 2020). This means that personal and sensitive data can be anywhere, including on technology assets that are no longer in use – putting agencies at enormous risk and with multiple challenges to mitigate that risk.

GOVERNMENT FOCUS ON INFRASTRUCTURE UPDATES

The Federal Government has recognized the need to dedicate funding to address the potential issues legacy systems impact the move to digital government, cyber security, data privacy and environmental concerns. To correct this, the Government of Canada (GC) is making significant investments to modernize and replace aging IT infrastructure and have adopted a "cloud-first" policy for government applications. Specifically, Budget 2021 announced $300 million of additional investments over 3 years for Shared Services Canada (SSC) to continue to work to repair and replace critical IT infrastructure.

The GC is looking to be more responsive to Canadians' demands for trusted and convenient services. An updated network will use the latest security measures that better protect personal information, connect seamlessly to cloud and enterprise data centres, and provide better connectivity.

50

Current Government of Canada (GC) networks across the country.

80%

of the GC's roughly 8,000 IT services are housed in aging data centres.

Foundational IT components of Digital Government, like networks and cyber security, will continue to be modernized.

The GC is making significant investments to modernize and replace aging IT infrastructure and have adopted a "cloud-first" policy for government applications.

The GC is working to identify, modernize and migrate key applications out of aging data centres and onto more secure and efficient modern hosting solutions, either on the cloud or in consolidated enterprise data centres.

Consolidating and modernizing is reducing the GC's carbon footprint.

SOURCE: https://www.canada.ca/en/government/system/digital-government/digital-government-strategy/what-we-doing/modernizing.html

SECURING INFORMATION WITH TECHNOLOGY DISPOSITION

Federal agencies are progressing in transitioning to a digital-first environment. This environment is evolving quickly due to the nature of technology proliferation. IT departments must remain ahead of the curve and can look to the following use cases to take a proactive approach.

DATA CENTERS

As cloud migration continues to increase, the reliance on government-housed data centers will substantially decrease, requiring appropriate disposition of equipment. The COVID-19 pandemic has only accelerated this focus. This trend will enable agencies to transition away from on-premises data center equipment, providing an opportunity to significantly consolidate the technology required in these environments leading to a significant volume of excess IT equipment.

OFFICE SPACE

SSC will reduce office spaces through modernization and optimization. The decrease in required office space, closing of offices and government buildings will require a strong look and assessment of the legacy technology equipment resulting in a significant opportunity to securely dispose of legacy assets.

HYBRID WORKERS

The hybrid workforce is expected to continue. Federal agencies will need to support the remote workforce with new or refreshed devices, disposing of the traditional in-office technology such as desktops, storage drives, printers and more.

INTELLECTUAL PROPERTY

Legacy hardware that stores intellectual property (IP), such as health-related research, geospatial data, contractual information, and patent/trademark applications are other candidates for secure ITAD. This technology must be securely removed, transported, and destroyed to ensure any IP information is wiped following strict guidelines.

ENVIRONMENTAL, SOCIAL AND GOVERNANCE

Agencies need innovative solutions that bring them closer to achieving their Environmental, Social and Governance (ESG) goals. Environmental solutions, in particular, allow the recycling process for technology assets to reduce greenhouse gas emissions, cut pollution and save energy and resources to improve green posture.

For every million cell phones recycled,

35,000

pounds of copper be recovered

Globally, only 9.7M tons of IT waste is recycled or remarketed annually (20%)

Recycling one million laptops saves the energy equivalent to the electricity used by more than 3,500 homes in one year.

A STRUCTURED APPROACH TO DISPOSITION

Outsourcing an ITAD program to an industry-leading third-party vendor with expertise in disposal can expedite the entire process and serve as a more economical use of agency resources. Agencies have traditionally performed ITAD as point-in-time projects, which come at higher prices than an established program. Third-party disposition of assets is cost-effective due to economies of scale, and can help long-term budgeting. Additionally, a comprehensive program can result in avoidance of fines and other costs associated with mismanaged ITAD.

A proper program should be viewed as a data security and environmental sustainability investment that adheres to a structured approach.

1. **Identifying sensitive data.** Understand which agency assets contain sensitive data and where these key assets are located.
2. **Establishing policies and procedures.** Implement consistent programs throughout the organization and monitor for compliance. It is crucial all employees are aware and understand the policies and procedures.
3. **Focusing on secure chain of custody.** Rather than a one-size-fits-all approach to processes and data sanitization methods, focus on security tailored to the nature of the data that includes tracking mechanisms to follow an asset from pick-up to destruction.

When an agency deploys a comprehensive disposition process and program, with a qualified third-party vendor, they can mitigate many concerns that can currently exist.

THE DANGERS OF IMPROPER ITAD

When federal organizations determine the need and secure the funding for ITAD, the first phase to moving forward in the disposition process is to consider several concerns from both an agency and third-party vendor perspective.

Negligence. It is both costly and time consuming to destroy data bearing IT assets, which provides an unfortunate opportunity of not adhering to regulations when disposing of IT equipment.

Human error. Internal employees or ITAD service providers cannot tell if data was properly sanitized simply by looking at the media on which it resides.

Improper handling. If the chain of custody is not verifiable, there is no way of knowing for sure whether equipment was diverted to a secondary market, landfill or elsewhere.

Environmental damage. If retired IT assets are not properly handled in an environmentally compliant manner, the agency faces incremental risk for fines, penalties and possible reputational harm. Focusing on meeting sustainability goals cost-effectively allows equipment to be managed in ways that reduce greenhouse gas emissions, cut pollution and save energy and resources.

By evaluating a strategic partner and ensuring a proper ITAD program is in place, federal agencies will be able to avoid the dangers and pitfalls of improper disposition.

MAXIMIZE PROTECTION AND VALUE

Proper evaluation of a strategic partner is critical to maximizing protection, compliance and value to federal organizations. Look for partners who comply with all regulations, industry best practices, and will legitimately dispose of IT assets. The onus to ensure data protection and environmental recycling practices ultimately falls to the government agency

MANAGE RETIRED IT EQUIPMENT

Disposition processes must be highly regimented and consistent. Agencies should have access to alternative destruction methods and locations: bulk or serialized media destruction and on-site or off-site destruction capabilities. Some organizations, such as defense or federal healthcare institutions, might not want any data-bearing devices to leave the premises – thus requiring an on-site data destruction solution.

AUDITABLE PROCESS AND WORKFLOW

Each item marked for disposal should be logged in an inventory and tracked through the entire disposal process. A best practice is to affix a scan code at the point of surrender and scan the tag at each hand-off point, allowing an agency to audit the process at any time. The inventory management system should flag any missing items and create an exception report.

SECURE LOGISTICS, TRANSPORTATION AND VEHICLES

Equipment is never more vulnerable than when it's in transit. Items can fall off open truck beds, and unlocked vans are an invitation to thieves. Look for ITAD providers that use closed, secured transportation and secure handoff points monitored by closed-circuit cameras.

PROOF OR CERTIFICATION OF DESTRUCTION

This is a document that verifies equipment has been scrubbed, recycled or destroyed in a manner that satisfies the terms of the contract. It's best to work with an ITAD vendor that has been certified by a respected third-party standards organization such as e-Stewards or Sustainable Electronics Recycling International.

COMPLIANT, ENVIRONMENTALLY SENSITIVE DISPOSAL

The provider should guarantee all IT assets are disposed of in an environmentally friendly manner that meets local, state and federal requirements. The provider's operations should adhere to widely recognized certification standards established by credible industry organizations, such as e-Stewards, R2 and RIOS.

COMPLIANCE FOR PROTECTED B DATA

There are many Federal government requirements for handling of data on IT assets.

Low-sensitive data, up to and including medium sensitive or **Protected B** data requires agencies to maintain a chain of custody of IT assets showing who has been in possession of the media/asset, and all actions taken with the media. This process begins when the asset is identified for sanitization, while the asset is being sanitized, during transportation to the authorized donation or disposal site, and up to and including its disposal.

Vendors who engage with the Federal Government on disposition of assets with Protected B data must have been previously authorized to handle such IT assets.

In additon to GC, Provincial, Municipal governments, Crown agencies and healthcare organizations can all benefit from the secure manner with which Iron Mountain handles such sensitive data.

CONCLUSION

With the continued growth of technology, disposing of devices securely and in a sustainable way is a priority for federal agencies. When transitioning to a digital-first environment, it is critical for agencies to protect their data and avoid the risk of a data breach. By having a comprehensive ITAD program, agencies can have insight on the status and security of all assets being disposed.

Working with a reputable third-party vendor to customize a comprehensive and secure ITAD strategy and program can reduce your risk and possibility of data loss by leveraging their experience and best practices. By investing the time and effort to create an ITAD program, agencies can help safeguard their IT assets and the data that is entrusted to them.

To talk to an ITAD representative of Iron Mountain Public Sector Solutions, email canada.goc@ironmountain.com

IRON MOUNTAIN®

PUBLIC SECTOR SOLUTIONS