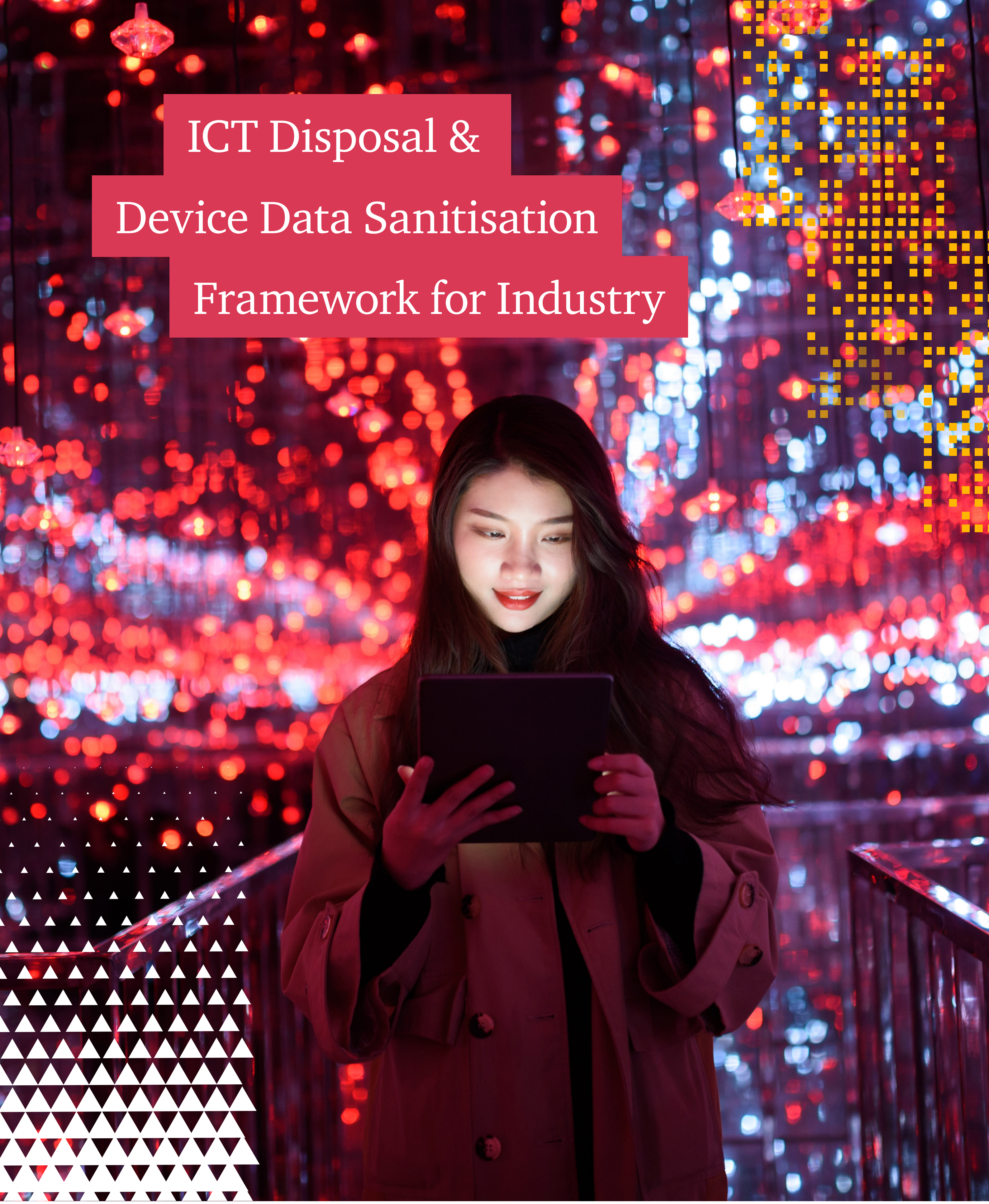
ICT Disposal & Device Data Sanitisation Framework for Industry



pwc

W TECHNOLOGIES

IT Disposals. A New Way.

Table of Contents

1 Executive Summary

In the digital age, the disposal of Information and Communication Technology (ICT) devices, often referred to as e-waste, is not merely an environmental concern but also a significant cybersecurity threat. Australian industry organisations dispose of millions of ICT devices annually, many of which still contain sensitive data. Improperly sanitised devices can be and are exploited by malicious actors, leading to catastrophic breaches of security and data privacy.

Key Concerns:

1. **Data Security Threats:** Unsanitised devices can expose sensitive information, including intellectual property, personally identifying information (PII), and network credentials, to cyber criminals.

2. **Environmental Impact:** E-waste contributes to environmental degradation, but its cyber implications are equally pressing.

3. **Legislative Gaps:** Current frameworks such as the Privacy Act 1988 and Security of Critical Infrastructure Act 2018 focus on live data security, leaving a gap in guidance, and mandates, for secure e-waste disposal.

Current Frameworks and Gaps:

1. **Essential 8, NIST CSF, AESCSF, and CPS234:** Provide controls for managing live data but lack specific directives for end-of-life data destruction.

2. **ISM and PSPF:** Offer detailed guidelines for government entities but leave private industry without clear mandates.

3. **Privacy Act 1988:** Imposes heavy fines for data breaches but lacks explicit requirements for secure disposal of data-bearing devices.

Risks of Data Breaches:

- It is estimated that 1 in every 250 devices is incorrectly disposed and contain data.

- Known data breaches from incorrect disposals aren't publicly known, but include multinational lawyers and retailers, Federal and State Government, Defence contractors, educational institutions, professional services firms, telecommunication providers among many others.

- Data breaches are increasing, with reports to the Australian Cyber Security Centre (ACSC) now made every seven minutes.

- The average cost of a data breach has risen significantly, making the financial and reputational risks of insecure disposal substantial.

Secure Disposal Methods:

- **Data Sanitisation:** Requires comprehensive procedures beyond just wiping hard drives. All data bearing points must be first checked, and all media sanitised or physically destroyed.

- **Destruction Methods:** Include degaussing, incineration, and disintegration/shredding. The method depends on the data sensitivity and device type.

- **Professional Services:** Utilising NAID AAA certified providers ensures compliance with rigorous standards for data destruction and handling.

Proposed Framework:

A robust framework for secure ICT disposal is essential. This framework recommends:

1. **Data Management Plans:** Identifying and managing data-bearing devices.

2. **Policy Development:** Ensuring only managed devices store data.

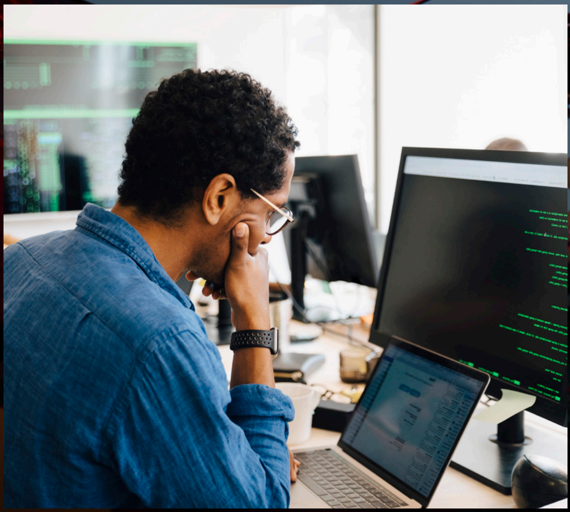
3. **Device Muster:** Keeping a comprehensive record of data-bearing devices.

4. **Certified Disposal Providers:** Using NAID AAA certified providers for sanitisation and destruction.

5. **Documentation:** Maintaining records of destruction for all data-bearing media.

The secure disposal of e-waste is a critical cybersecurity issue. Given the increasing penalties for data breaches, organisations must adopt rigorous disposal practices. By following a structured framework, entities can mitigate risks, comply with regulations, and protect sensitive information effectively. This approach aligns private sector practices with government standards, enhancing Australia's overall cybersecurity posture.

2 Why be concerned about ICT disposals?



Every year, Australian organisations dispose of millions of ICT devices, most often referred to as e-waste. However, the term e-waste confines the issue to waste, when the problem is both a cyber security and environmental issue. The data stored on these devices and their components mayoften contain sensitive information related to an organisation's operations and intellectual property, as well as personally identifying information (PII) and in the case of networking devices may provide access to credentials for entire networks. And if they end up in the hands of a malicious actor, the results could be catastrophic. It is estimated that approximately 1 in every 250 devices disposed of are not properly sanitised.

The insecure disposal of ICT devicese-waste, which remains a peripheral issue in the cybersecurity space, presents serious cyber and data security threats to Australian organisations and citizens. Notably, in the context of Australia's critical infrastructure regime, which has undergone significant reforms, there exists no explicit obligation for captured entities to securely dispose of e-waste.

Currently, frameworks or industry requirements discuss data destruction broadly, intending to covers both digital and physical assets. Paper based asset destruction have very specific requirements and controls. Digital Data that is "live" in systems is the focus of security focussed legislation such as the Privacy Act 1988 and the Security of Critical Infrastructure Act 2018 which impose heavy fines and penalties for entities that suffer data breaches and there is extensive advice available as to how to manage security of data in existing 'live' systems. Digital data doesn't disappear from hardware at the end of its lifecycle, however Australia doesn't currently have legislation or frameworks to guide a best practice approach to guide industry and individuals to manage hardware and the data it contains at the end of its life.

Current cybersecurity frameworks such as the Essential 8, NIST CSF, AESCSF and CPS234 speak to the cyber practices required to keep 'live' data safe and provide controls for management of devices. For example APRA-regulated entities which hold sensitive PII and protected health information (PHI), are required to follow the CPS 234 information security policy framework to ensure that information security is considered at each stage of the lifecycle of an asset (from acquisition through to decommissioning and destruction). However, for scenarios where entities have data stored on devices that are no longer in use, there is a gap in specific advice on how to manage an appropriate destruction level.

Whilst the Government has specific controls within the Information Security Manual (ISM), and the Protective Security Framework (PSPF) that guide the required destruction procedures for various classifications of data, private industry and individuals have no such specific mandates. This report analyses the controls provided in the ISM, PSPF, AESCSF and CPS234 amongst others to propose a framework for industry and individuals to apply when deciding how and when to destroy a device that has held sensitive data. It is important to note that this report specifically addresses digital data (e-waste) destruction and does not encompass the disposal of paper-based assets, which may entail separate and specific requirements for the secure destruction of information.

This fills a significant gap in guidance for industry and supports an 'all-hazards' approach to cybersecurity risks and further bolster the cybersecurity of Australia - particularly critical infrastructure entities.

It would also align the cybersecurity requirements of captured entities with the provisions that Australian Government entities are required to adhere to under the Protective Security Policy Framework (PSPF), Information Security Manual (ISM) and Australian Prudential Regulation Authority (APRA) . More broadly, with the introduction of significant fines for serious or repeated privacy breaches now in force under the Privacy Act 1988 (Cth) (Privacy Act), captured entities must also be aware of this looming data security threat and take steps to ensure the secure disposal of e-waste to better protect PII.

What is e-waste?

As defined by The Global E-waste Statistics Partnership, e-waste is: "All items of electrical and electronic equipment and its parts that have been discarded by its owner as waste without the intent of re-use. Data that remains on devices destined for re-use poses the same threat if not disposed of correctly. E-waste is also referred to as WEEE (Waste Electrical and Electronic Equipment), electronic waste or e-scrap in different regions and under different circumstances in the world. It includes a wide range of products – almost any household or business item with circuitry or electrical components with power or battery supply".[1] The most recent figures available indicate that in Australia and New Zealand about 650 kilotons of e-waste is produced annually and, of this, only 59 kilotons is formally collected - about 10 per cent.[2]

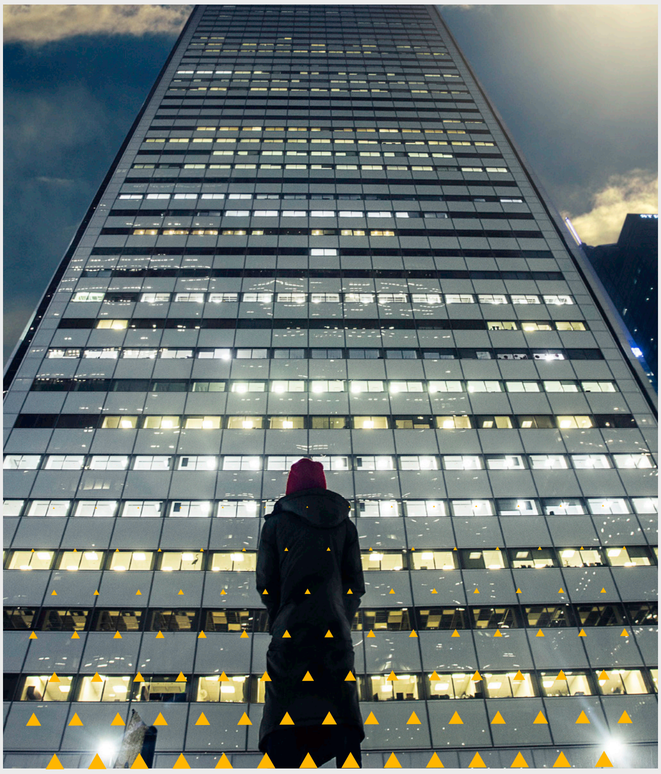
While the detrimental environmental implications of e-waste have been widely explored, the serious cybersecurity risks associated with data retained on discarded devices have not. This is an area that needs urgent attention given predicted future trends - it is estimated by 2030 the volume of global e-waste will exceed 70 million tonnes per year.[3] This increase is largely due to the rapid proliferation and turnover of Internet of Things (IoT) devices. It is estimated by 2030 there will be more than 25 billion IoT devices globally[4] - and these devices continue to expand the amounts of valuable sensitive data they store.

[1] Global E-waste Statistics Partnership
[2] Country Sheets: Australia and New Zealand
[3] E-waste surges in 2021 as world sends goldmine to landfill - ABC News
[4] Internet of Things statistics for 2022 - Taking Things Apart

What is the risk of loss of sensitive data from devices?

The simple fact is that entities not taking all reasonable steps to sanitise data bearing devices which hold sensitive information appropriately are not effectively managing the risk of data breach. In Australia, taking all reasonable steps is achieved by having significant internal control mechanisms including skilled personnel able to perform scans and data sanitisations, record generation and management and potentially specialist equipment for device destruction. Alternatively, entities can use an appropriately certified IT disposals partner (NAID AAA certified with PSPF Endorsement to the appropriate level), with appropriate transport/ logistics and with appropriately cleared personnel throughout the chain of custody of the end-of-life IT equipment (we provide a view of the detailed process in our framework table in section 2).

In November 2022, the Australian Government increased the fine for data breaches from AUD $2 million to AUD $50 million, 30% of company revenue or three times the benefit from any value of the use of the information . These serious fines recognise that responsible data management is expected from all Australian companies and entities and that data breaches must be prevented so far as is reasonably possible. Reported figures of expected cyber spend range from 6-10% of IT budgets and efforts to secure data as part of this investment principally focus on data that is "live" in a system. Few companies show effective cybersecurity controls to manage data in devices that are disposed of. Data breaches will attract fines regardless of whether the data is lost in a disposed device or in a live system. Reputationally speaking, companies should also be conscious of moves by the Australian Institute of Company Directors and the Australian Securities and Investment Commission to recognise that prosperous and effective cybersecurity has become part of the normal practice of all companies.



The direction shows less tolerance for cybersecurity breaches and a greater level of scrutiny on the role of Boards in supporting responsible cybersecurity practices. The proper disposal of data in devices is one simple, but often overlooked part of this practice.

Recent figures from the Australian Cyber Security Centre's (ACSC) shows that reports on data breaches are now made every 7 minutes, up from every 8 minutes the previous year.[6] According to IBM, the average cost of a data breach worldwide will be USD $4.45 million in 2023, up 15% from 2018.[7] These figures indicate that the risk, as determined by your risk matrix, is likely to fall within the moderate to high range. Significant data breaches occur at least every few months making that risk likelihood quite high and the consequences of even a small loss of data are significant when fines in the magnitude of millions are in play.

[5] Attorney Generals Department press release
[6] ACSC Annual Cyber Threat Report, July 2021 to June 2022
[7] Critical Cyber Crime Statistics in Australia 2023

What is secure disposal?

Secure disposal of e-waste is complex – as IT devices continue to advance, it is increasingly about much more than just wiping hard drives. Internal policies and guidance may over-simplify or overlook the detail and complexity required in appropriately disposing of a device. A simple check on IT Security Policy for device disposal may be a good first step for technology leaders seeking to assess whether poor data sanitisation may be a threat.

A policy that states "appropriate" disposal considerations be made without further specifying the use of a provider and/or a specific owner to manage device destruction may leave staff in the unenviable position of being responsible for data sanitisation but absent the mechanisms to perform it effectively. For example, when it comes to devices holding sensitive information or access credentials to networks, professional disposal by a National Association for Information Destruction AAA (NAID AAA) certified provider with the appropriate level of PSPF Endorsement should be considered and may even be mandatory.

If there is an intention to re-sell used devices, then organisations should ensure that all data bearing media in the device has been properly sanitised. Again, requirements vary from device to device and depend on the sensitivity level of the data. However, most people, including cybersecurity professionals, are still not aware that data is held in areas other than just the hard drive or solid-state drive. For example personal devices such as laptops generally hold data across 7-12 points (EEPROM/Firmware, SSD/HDD, Second SSD/HDD, Optical, USB, SIM, Wi-Fi Card, SD/Micro), whereas a network device can require sanitisation across up to 30 data bearing points including lesser known, but critically important, media such as Cache Cards, Remote Access Chips, FPGA, Lifecycle Controller, RAID, EEPROM/PROM/EPROM chipsets and in general configuration files in the firmware.

Where any of these data bearing points cannot be confirmed as properly sanitised, they should be removed and properly destroyed in accordance with the risk level. Furthermore, any identifying marks or stickers on the device should be removed.

Where complete certainty of effective sanitisation cannot be verified, then data bearing media must be destroyed using one of the approved methods of destruction. Again, this will depend on the media type and the risk/sensitivity level of the data held on the device or storage media. For some storage media such as older magnetic hard drives and storage tapes, an approved degausser can be used. Degaussing magnetic media using a coercive magnetic force changes its properties, which results in data being permanently corrupted and rendered unrecoverable.[8]

However, coercivity is variable between magnetic media types, brands, and models, meaning attention must be paid to the strength of the magnetic field that is applied. If it is not strong enough, data may be retained on a device and, therefore, recoverable.[9] A degausser from the US Evaluated Products List[10] with a minimum of 30000 gauss field strength across dual directions and with a minimum Coercivity rating of 3000 Oersted's and which is properly calibrated can be used.

Other approved destruction methods include incineration and disintegration/shredding/granulation for higher security levels. Where devices are assessed as holding highly sensitive information, media should be shredded into 3-6mm pieces and <3mm pieces for high-security data (see table below for more details).

Developing internal processes to comprehensively address the various areas where data may reside for all devices in use by an entity will be a significant undertaking and – if performed in house - may involve the acquisition, maintenance and operation of specialist equipment as indicated above. Entities seeking to show an effective control for the proper disposal of devices bearing data, the simplest and most cost-effective solution will be to develop a simple process as follows:

1. have a data management plan that identifies data bearing devices and components of these devices,
2. have a policy on device use - ideally that only managed devices be used to store data,
3. maintain a muster of company owned devices - these should correspond to the data management plan so that picture of data bearing devices is available,
4. require that data bearing devices use a NAID AAA certified provider for sanitisation and destruction, and
5. obtain and record the record of destruction from the NAID AAA for each mustered device and each data bearing point/media.

This approach means that, should a data breach occur - company directors and executives can demonstrate that the breach did not occur due to the failure to properly dispose of a data bearing device.

[8] https://www.cyber.gov.au/sites/default/files/2021-12/14.%20ISM%20-%20Guidelines%20for%20Media%20%28December%202021%29.pdf

[9] Degausser | Cyber.gov.au

[10] https://www.nsa.gov/portals/75/documents/resources/everyone/media-destruction/NSAEPLMagneticDegaussersApril2021.pdf?ver=FIfD6KRhBVf1D3cXepQ3ag%3D%3D

PSPF and ISM obligations

There is a gap in guidance for industry on specifically how to dispose of data bearing devices and media securely. Most cybersecurity frameworks such as the AESCSF, NIST CSF and the ISO 27001 identify that data on devices should be sanitised "appropriately" but the next logical step of what is an appropriate level of disposal is not defined. This makes it hard for industry to understand if they have done a "good enough" job and taken "reasonable steps" to protect their sensitive data.

The Australian Government's information security framework is captured in two documents - Protective Security Policy Framework (PSPF), which is administered by the Attorney-General's Department, and the Information Security Manual (ISM), which is administered by the Australian Signals Directorate (ASD). Further, the Security Construction and Equipment Committee (SCEC) provides guidance on equipment, transport, and ASIO T4 which has outsourced IT destruction oversight to NAID.

The Protective Security Policy Framework (PSPF) sets out the requirements Australian Government entities must abide by in relation to protecting information and assets. One of its four pillars relates to information security. According to the PSPF, "entities must ensure security classified information is stored, transferred, and disposed of appropriately".[11] The PSPF guidelines mandate that procedures and processes contained within the ISM should be followed for the purposes of secure disposal.[12] Further, many organisations which hold Government contracts and therefore data, must also follow the PSPF which is likely written into service contracts.

The ISM contains strict and prescriptive conditions for the disposal of redundant devices storing sensitive information. It states that: "Before ICT equipment can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed, or declassified ICT equipment still presents a security risk, albeit very minor, an appropriate authority needs to formally authorise its release into the public domain. Furthermore, as part of disposal processes, removing labels and markings indicating the owner, sensitivity, classification, or any other marking that can associate ICT equipment with its prior use will ensure it does not draw undue attention following its disposal".[13]

The ISM outlines that, for secure destruction of materials from OFFICIAL up to SECRET (below TOP SECRET) classification, a National Association for Information Destruction AAA (NAID AAA) certified destruction service, with the appropriate level of NAID certification and PSPF endorsement must be used.[14] NAID AAA certified destruction facilities are independently audited to ensure stringent protocols are in place to ensure the security of confidential material throughout all stages of the destruction process such as handling, transporting, storing materials prior to destruction and destroying and disposing of materials responsibly.[15] It also notes that the destruction of devices storing highly sensitive data should be supervised by at least two personnel, who also sign a destruction certificate afterwards.[16] While the ISM does not specify that a NAID supplier must be used for performing sanitisation, it can be considered implied because sanitisation frequently fails and subsequent destructions must occur even if sanitisation is the first preference for a particular device or media type. In this case, a NAID certified company which is also certified for sanitisation (as well as destruction) should be used.

Further, the PSPF, SCEC and the ISM along DISP (for Defence Industry) provides for certain controls over the logistics methods, handling and level of AGSVA security clearances required from any personal working on the disposal and sanitisation of end-of-life IT equipment.

In summary, using a NAID Certified Supplier with the appropriate level of certification and PSPF endorsements which also has the correct logistics process and appropriately AGSVA cleared staff is the most effective way to ensure that any organisation is taking all reasonable steps to protect sensitive information.

[11] Policy 8: Sensitive and classified information
[12] https://www.protectivesecurity.gov.au/system/files/2023-01/pspf-policy-08-sensitive-and-classified-information.pdf
[13] Information Security Manual (ISM) | Cyber.gov.au, P71
[14] Ibid 13, P81
[15] NAID AAA Certification in Canberra | Shred-X
[16] Ibid 13, P80

What does this mean for Industry?

Over the past several years there has been significant cyber-related legislative and regulatory focus in Australia and this trend is set to continue. This year has seen the release of the 2023-30 Australian Cyber Security Strategy, which discussed broadening the SOCI Act 2018 (Cth), hardening government systems, and ongoing consultation into Privacy Act reform, aimed at ensuring Australia's privacy laws are fit for the digital age. It also provides the Office of the Australian Information Commissioner (OAIC), Australia's privacy regulator, with greater powers to resolve privacy breaches and strengthens the Notifiable Data Breaches scheme to ensure the OAIC has comprehensive knowledge and understanding of information compromised in a breach, so risk of harm to individuals can be better assessed.[17]

This trend shows greater strengthening on what has already been a consistent message of requiring greater ownership of data protection by industry. The Australian Privacy Principles are already explicit on data protections, (APP) 11.2 states that entities must "take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs". Furthermore, the OAIC's Guide to Securing Personal Information (the Guide) notes that "destroying or permanently de-identifying personal information that you no longer need is an important risk mitigation strategy".[18] While the Guide does present a series of useful questions for organisations to consider in dealing with destroying data (including that contained on redundant devices), it does not present a binding or prescriptive guidance for organisations to follow, especially smaller organisations.

APP11.37 footnotes the ISM when discussing what taking "reasonable steps" includes, which implies that following the ISM could be considered as taking reasonable steps. By extension, given that the ISM states that a NAID certified supplier must be used for destruction, it may be worth considering for organisations which hold sensitive information.

Given the expected changes to the Privacy Act - and the significant fines now in place - secure disposal of e-waste should also be a primary concern for organisations deemed critical infrastructure and/or captured by the Privacy Act 1988. In particular, this should capture the attention of organisations holding significant amounts of PII and sensitive information like retailers, professional services providers and not-for-profits. For such organisations, data security should be front of mind and include provisions for the sanitisation or secure disposal of e-waste.

[17] Ibid 23
[18] Guide to securing personal information - Home

Conclusion

As the systems and functions society relies upon become ever-more digitised, serious consideration must be given to how the vast amounts of e-waste, and the valuable data they hold, is securely disposed of.

There is no doubt that amid an increasingly complex regulatory and legislative cybersecurity backdrop, organisations are making big changes to the way they protect data during its lifecycle. But, as this report explores, there are significant risks posed by unsanitised e-waste and, anecdotally, there is clear evidence poor sanitisation and destruction practices are widespread. Hence, there is an urgent need to, as a first step, ensure that Australia's critical infrastructure entities are required to securely dispose of redundant devices.

Furthermore, with the introduction of significant penalties for "serious or repeated" breaches of the Privacy Act, this is an issue that requires attention more broadly across the economy.

Given virtually all organisations in any sector will hold some level of sensitive information, the recommended approach to complete compliance when retiring IT equipment is to use a NAID AAA certified IT disposals/destruction company with the appropriate level of PSPF endorsements that also has the appropriate logistics solutions in place and appropriately security cleared personnel for the assessed level of sensitivity of the data on the equipment.

To this end, we have developed a framework to support responsible, accountable, and auditable decision making for the secure disposal of redundant devices for organisations captured by the *Privacy Act 1988, the Security of Critical Infrastructure Act 2018* or other legislation. This framework supports companies to show due diligence and responsible destruction of devices designed to support both large firms and small and medium enterprises, which have more limited resources and expertise to support secure disposal practices.

3

Data Sanitisation Framework

Objective

This framework supports companies to show due diligence and responsible destruction of devices designed to support both large firms and small and medium enterprises, which have more limited resources and expertise to support secure disposal practices.

Framework

Data Classification and Recommended Disposal

Equivalent Government Data Classification	Impact statement for loss/breach and relevant legislation	Probable Equivalent Industry Data Classification	Adapted Impact Statement	Liability Impact	Proposed Destruction Method, Transport and Handling and Personnel
Unofficial	No damage. This information does not form part of official duty	Public E.g., press releases, website, marketing materials, and publications. *Note – it is unlikely an IT device would **only** contain public data.	Nil or Low No damage. This information is authorised for public dissemination. *Note – it is unlikely an IT device would **only** contain public data.	Nil or Low Possible reputational damage if items are found in inappropriate location as owner would be known.	**IT disposal partner must be:** No requirement, however, as it is unlikely that any IT device will hold **only** public facing data then it is prudent to treat as **official.** **Personal Devices (Laptops/Mobile etc)** **Sanitisation/Destruction:** No requirements if this is public facing data only. However, as it is unlikely that any IT device will hold **only** public facing data then it is prudent to treat as **official** and run an ISM compliant overwrite on the HDD/SSD (e.g. overwrite with verified readback), reset Bios, remove any other storage devices (optical, USB, SD, SIM etc), remove any identifying external tags. **Destruction:** Any storage media which fails overwrite and/or readback to be made inoperable, however due to the low likelihood of any IT equipment holding only **Unofficial** equivalent data then it may be prudent to follow process for **official** and destroy using ISM approved destruction method. (i.e., Disintegration/Shredding/Incineration or NSA Evaluated Product List approved Degausser for magnetic media. **Transport and Handling:** No requirements, however due to the low likelihood of any IT equipment holding only **unofficial** equivalent data then it may be prudent to follow process for **official** and have secure transport. **Personnel Requirement:** No Requirements, however due to the low likelihood of any IT equipment holding only **unofficial** equivalent data then it may be prudent to follow process for **official** and use police cleared personnel only, or locked cages with tamper proof seals, or AGSVA Baseline cleared personnel only. **Notes on Other Devices Z(Networking/Servers).** As above **Notes on Other Devices (Printers/MFP etc.)** As above

Framework cont

Data Classification and Recommended Disposal

Equivalent Government Data Classification	Impact statement for loss/breach and relevant legislation	Probable Equivalent Industry Data Classification	Adapted Impact Statement	Liability Impact	Proposed Destruction Method, Transport and Handling and Personnel
Official	No or insignificant damage. This is the majority of routine information.	**Internal non-sensitive** E.g., publicly known project planning documents, or benign documents such as inventory records. i.e. no personal information, employee records, private names, phone numbers, intellectual property etc Note: any organisation that contracts with the Federal Government and this involves **official** level information will be required to adhere to the PSPF.	**Low/med** Routine company information which if released would not cause any personal or company sensitive information to be released.	As above, with further possible reputational damage if company or personal information of limited sensitivity was also on devices. Possible insurance coverage issues or certification breaches (27001, DISP or other).	**It disposal partner: must be:** NAID AAA Certified (Aust Regime) Personal Devices (Laptops/Mobile etc) **Sanitisation/Destruction:** ISM compliant overwrite on the HDD/SSD (e.g., overwrite with verified readback), reset Bios, remove any other storage devices (optical, USB, SD, SIM etc), remove any identifying external tags. **Destruction:** Any storage media which fails overwrite and/or readback to be made inoperable. **Transport and Handling:** Data at this level should be handled at the discretion of the data owner depending on the data risk type. It is unlikely that an IT asset would hold internal **official** equivalent information and not also hold any sensitive information (i.E., Personal/ employee information of any kind, or company information that could damage the organisation if leaked), so handling according to **official sensitive** may be prudent. **Personnel Requirement:** Data at this level should be handled at the discretion of the data owner depending on the data risk type. It is unlikely that an IT asset would hold internal **official** equivalent information and not also hold any sensitive information (i.E., Personal information of any kind, or company information that could damage the organisation if leaked), so handling according to **official sensitive** may be prudent. **Notes on Other Devices (Networking/ Servers).** As above for Laptops/Phones Data at this level should be handled at the discretion of the data owner depending on the data risk type. It is unlikely that an IT asset would hold internal **official** equivalent information and not also hold any sensitive information (i.E., Personal information of any kind, or company information that could damage the organisation if leaked), so handling according to **official sensitive** may be prudent. Networking devices can be extremely complex as they store data and access credentials in many places (chipsets and adapter cards for example) other than just the hard drive or flash cards and these must be verified as sanitised or made inoperable. **Notes on Other Devices (Printers/MFP etc.)** Factory Reset, if fails then make inoperable. Check for paper jams for sensitive papers and destroy if found

Framework cont

Data Classification and Recommended Disposal

Equivalent Government Data Classification	Impact statement for loss/breach and relevant legislation	Probable Equivalent Industry Data Classification	Adapted Impact Statement	Liability Impact	Proposed Destruction Method, Transport and Handling and Personnel
Official - sensitive	Limited damage to an individual, organisation or government generally if compromised.	**Commercial/ sensitive** **Personnel in confidence** E.g., intellectual property records and patents, sensitive customer data, employee health records, employee contracts and agreements, customer lists, personal addresses/phone numbers. Note: any organisation that contracts with the Federal Government and this involves **official sensitive** level information will be required to adhere to the PSPF.	**Moderate/high** If disseminated in an uncontrolled or unauthorised manner may constitute a breach of the Privacy Act or the SOCI Act 2018 and is reportable to the NDBS and/ or the ACSC. Not authorised for dissemination outside the organisation. May trigger ASIC, ASX, APPRA, GDPR or other regime mechanisms or penalties. May support negligence or other claims against directors/officers and or company.	May be a reportable offence. Possible damage to personnel privacy, supports threat actors to attack the entity. May trigger ASIC, ASX, APPRA, GDPR or other regime mechanisms or penalties. Likely insurance coverage issues or certification breaches (27001, DISP or other). May support negligence or other claims against directors/officers and or company	**It disposal partner: must be:** NAID AAA Certified (Aust Regime) With PSPF Endorsement (level 1 Official Sensitive) **Personal Devices (Laptops/Mobile etc)** **Sanitisation/Destruction:** As for **official** **Destruction:** As for OFFICIAL, however when shredding/ disintegrating then this should be done so that ALL resultant particles are <16mm and if degaussing an NSA Evaluated products list Degausser with appropriate field checking procedure implemented. **Transport and Handling** Secure transport with vetted drivers and handlers only, or lockable vessels with tamper evident seals to prevent access. **Personnel Requirement:** A minimum requirement may be police cleared personnel only, or locked cages with tamper proof seals, or AGSVA Baseline cleared personnel only depending on data risk type. **Notes on Other Devices (Networking/ Servers).** Networking devices can be extremely complex as they store data and access credentials in many places (chipsets and adapter cards for example) other than just the hard drive or flash cards and these must be verified as sanitised or destroyed. **Sanitisation of Network Device Other Storage Media** (inexhaustive list of examples): Sanitise: Lifecycle Controller Card Sanitise: Remote Access Cards Sanitise: Hardware Cache Cards Sanitise: RAID configured storage Reset: Configuration Numerous other device-specific processes may be required (i.e reset IDRAC, Host Shutdown etc.) Where any of these processes cannot be 100% verified, then if the card/media can be removed from the device it should be made inoperable, if not then the whole device should be made inoperable. **Notes on Other Devices (Printers/MFP etc.)** Factory Reset, if fails then remove and destroy storage devise (shred < 16mm). Check for paper jams

Framework cont

Data Classification and Recommended Disposal

Equivalent Government Data Classification	Impact statement for loss/breach and relevant legislation	Probable Equivalent Industry Data Classification	Adapted Impact Statement	Liability Impact	Proposed Destruction Method, Transport and Handling and Personnel
Protected	Damage to the national interest, organisations or individuals.	**Restricted commercial/ personnel** E.g., classified financial records, confidential legal documents related to litigation, more sensitive intellectual property (secret trade formulas, processes, client lists etc.) Any data/device which could pose a risk to critical infrastructure or other national security interests. Note: any organisation that contracts with the federal government and this involves **protected** level information will be required to adhere to the PSPF.	**High** Sensitive PII or SOCI Protected information. If disseminated in an uncontrolled or unauthorised manner constitutes a breach of the Privacy Act or the SOCI Act 2018 and is reportable to the NDBS and/or the ACSC. Access controls apply within the organisation. Not authorised for dissemination beyond the existing access holders and not authorised for dissemination outside the organisation. May trigger ASIC, ASX, APPRA, GDPR or other regime mechanisms or penalties. May support negligence or other claims against directors/officers and or company.	Damage to personnel privacy, supports threat actors to attack the entity. A reportable offence. Fines and penalties under the Privacy Act 1988 of a maximum of $2,500,000 for an individual and $50,000,000; or three times the value of the benefit obtained directly or indirectly; or if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention and the SOCI Act 2018 of $11,100 to $55,500 per offence. May trigger ASIC, ASX, APPRA, GDPR or other regime mechanisms or penalties. Likely insurance coverage issues or certification breaches (27001, DISP or other). May support negligence or other claims against directors/officers and or company.	**It disposal partner: must be:** NAID AAA Certified (Aust Regime) With PSPF Endorsement (level 1 Official Sensitive) **Sanitisation:** As for **official sensitive** with the additional requirements below: **Destruction:** When shredding/disintegrating that **All** resultant particles should be < 9mm **Transport and Handling:** Secure transport with cleared personnel and/or lockable vessels with tamper evident seals. **Personnel:** Minimum AGSVA Baseline cleared personnel supervision.

Framework cont

Data Classification and Recommended Disposal

Equivalent Government Data Classification	Impact statement for loss/breach and relevant legislation	Probable Equivalent Industry Data Classification	Adapted Impact Statement	Liability Impact	Proposed Destruction Method, Transport and Handling and Personnel
Secret	Serious damage to the national interest, organisations or individuals.	Highly Sensitive: Entities working on high security projects and some critical infrastructure may align their risk levels with **secret.** NOTE: any organisation that contracts with the Federal Government and this involves **secret** level information will be required to adhere to the PSPF.	As above with more catastrophic consequences	As above with more catastrophic consequences	**It disposal partner: must be:** NAID AAA Certified (Aust Regime) With PSPF Endorsement (level 2 Secret/Top Secret) **Sanitisation:** **No sanitisation only allowed.** Sanitisation may be used as an additional step prior to destruction, but all devices and media must be **destroyed only.** **Destruction:** When shredding/disintegrating that **all** resultant particles should be < 3mm Note: Any data bearing part of a device must be shredded to < 3mm which includes motherboards and adapter cards as they contain EEPROM, FPGA, PROM etc. chipsets. **Transport and Handling:** Secure transport with NV1 cleared personnel and lockable vessels with tamper evident seals. **Personnel** Minimum AGSVA NV1 cleared personnel supervision **Notes on Other Devices (Networking/ Servers).** Motherboard, storage media and all adapter cards must be shredded to <3mm **Notes on Other Devices (Printers/MFP etc.)** Plattne, rollers, any chipsets and motherboards must be shredded to <3mm
Top secret	Exceptionally grave damage to the national interest, organisations or individuals.	Extremely Sensitive: Entities working on very high security projects and some critical infrastructure may align their risk levels with **top secret.** Note: any organisation that contracts with the federal government and this involves **top-secret** level information will be required to adhere to the PSPF.	As above with exceptionally catastrophic consequences	As above with exceptionally catastrophic consequences	Not to be outsourced however if external facilities are used then two NV2 cleared personnel with supervision from data owner **must** be provided for all processes. As for **secret** with all destruction to <3mm particle size

Summary

The above table shows that because virtually every IT device will hold some level of sensitive information then the risk of a minimum $50 million fine exists for a data breach.[19] Therefore, virtually every device should be treated in accordance with controls governing either **official sensitive** (for lower risk e.g. some SMEs and Medium companies, Local Councils, some NFP's, Schools etc) or **protected** (for higher risk e.g. Medical Services, Law/Accountants, Tech companies, Insurance, Banks, some NFP's or SME/Medium Companies with higher sensitivity information) control requirements under the PSPF or ISM frameworks. Where there is extreme risk to national security or the community (such as critical infrastructure for example), then some devices may be assessed as being treated in line with **secret** level control requirements. These controls all require a level of destruction of data best managed by certified providers and/or with a dedicated in-house capability that may require significant outlay to implement.

[19] e.g. PII – name, phone, address etc of client or employee, or email threads, or company information.

Approach

Existing controls for data management and specifically device destruction have been taken from the Government advisories - the Information Security Manual and the Protective Security Framework as well as industry applicable frameworks for information security.

The controls in these frameworks are aligned to Government classification regimes which have been adapted for industry use leveraging fines and penalties associated with relevant legislation such as the *SOCI Act 2018 and the Privacy Act 1988* to determine industry relevant data types for treatment. Together - the controls and the data classifications identify two tiers for device destruction with corresponding guidance on what processes would constitute responsible, evidentiary destruction of the data bearing device.

Methodology

The framework is a mechanism by which to determine what kind of data your device is holding and what level of destruction or sanitisation is recommended by identifying alignment with key controls from Government and other frameworks for best practice information security. To use the framework;

1. identify what applicable framework and controls best represent your use case as a user using column C,
2. look at the equivalent key controls from that framework using column D, and
3. use the decision tree to determine whether a NAID certified provider should be used or whether internal processes are sufficient.

A.No.	B. Framework	C. Use Case	D. Key Controls
1	Information Security Manual: The Information Security Manual developed by the Australian Cyber Security Centre (ACSC), provides a cybersecurity framework that organisations can utilise within their risk management framework to protect their systems and data from potential cyber risks. This manual serves as a reference guide for employees and cybersecurity professionals on how to handle, store and transmit sensitive data securely.	Data within Government systems including highly classified systems.	ISM-0371: Personnel supervising the destruction of media supervise its handling to the point of destruction and ensure that the destruction is completed successfully. ISM-1741: ICT equipment destruction processes, and supporting ICT equipment destruction procedures, are developed, implemented and maintained. ISM-1742: ICT equipment that cannot be sanitised is destroyed. ISM-0312: ICT equipment, including associated media, that is located overseas and has processed, stored, or communicated. AUSTEO or AGAO data that cannot be sanitised in situ, is returned to Australia for destruction. ISM-0315: High assurance ICT equipment is destroyed prior to its disposal. ISM-1217: Labels and markings indicating the owner, sensitivity, classification, or any other marking that can associate ICT equipment with its prior use is removed prior to its disposal. ISM-0321: When disposing of ICT equipment that has been designed or modified to meet emanation security standards, the ACSC is contacted for requirements relating to its disposal. ISM-0316: Following sanitisation, destruction or declassification, a formal administrative decision is made to release ICT equipment, or its waste, into the public domain. ISM-0370: The destruction of media is performed under the supervision of at least one person cleared to its sensitivity or classification. ISM-0371: Personnel supervising the destruction of media supervise its handling to the point of destruction and ensure that the destruction is completed successfully. ISM-0372: The destruction of media storing accountable material is performed under the supervision of at least two personnel cleared to its sensitivity or classification.
	Protective Security Policy Framework: The Protective Security Policy Framework (PSPF): Australian Government entities to protect their people, information, and assets, both at home and overseas. It sets out government protective security policy and supports entities to effectively implement the policy across security governance, information security, personnel security, and physical security.		Policy 8, Requirement 8: Disposal Entities must ensure sensitive, and security classified information is disposed of securely in accordance with the minimum protection requirements set out in Annexes A to C. This includes ensuring sensitive and classified information is appropriately destroyed when it has passed minimum retention requirements or reaches authorised destruction dates. See C-5-71 for further details on appropriate commercial entities for use in destruction and engagement of same.

Methodology cont.

A.No.	B. Framework	C. Use Case	D. Key Controls
	CPS/CPG 234: CPS 234 is a regulatory framework issued by the Australian Prudential Regulation Authority (APRA) that sets out cybersecurity standards for APRA-regulated entities, including financial institutions. It mandates the implementation of robust information security controls, governance, and incident response mechanisms to protect sensitive financial and customer data from cyber threats. CPG 234 complements CPS 234 by providing additional guidance and best practices for APRA-regulated entities to enhance their cybersecurity frameworks and incident management capabilities. It assists these organisations in effectively implementing the requirements outlined in CPS 234 to better protect sensitive financial and customer data.	APRA-regulated entities including financial institutions, superannuation funds and insurance companies	CPS 234 (21): An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with: (a) vulnerabilities and threats to the information assets; (b) the criticality and sensitivity of the information assets; (c) the stage at which the information assets are within their life-cycle;9 and (d) the potential consequences of an information security incident. CPS 234(22) Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity. CPG 234 (37): Decommissioning and destruction controls are typically used to ensure that information security is not compromised as information assets reach the end of their useful life. Examples include archiving strategies and the secure data deletion (that is, deleting data using techniques to ensure data is irrecoverable) of sensitive information prior to the disposal of information assets.
2	ISO 27001: The international gold standard for information security management. It is used to prove the strength of your security posture to prospects and customers in global markets.	Industry focussed information security standard.	A.8.3.1: Procedures shall be implemented for management if removable media in accordance with the classification scheme adopted by the organisation A.8.3.2: Media shall be disposed of securely when no longer required, using formal procedures A.8.3.3: Media containing information shall be protected against unauthorised access misuse or corruption during transportation A.11.2.5: Equipment, information and software shall not be taken off-site without prior authorisation A.11.2.7: All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. A.11.2.9: A clear desk policy for papers and removable storage media and clear screen policy for information processing facilities shall be adopted A.18.1.4: Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable
	AS/NZS 5377: The AS/NZS 5377 standard was developed by the Australian Government's Department of the Environment, and the New Zealand Ministry of Environment to provide a uniform approach to assessing e-waste management systems.		1.5: Legal regulatory and international requirements that apply directly to end-of-life electrical and electronic equipment should be identified and adhered to, and information on these requirements should be kept up to date and communicated to relevant stakeholders. 1.6.1: Management of electrical and electronic equipment should be integrated to an organisation's existing environmental management system to encourage effective implementation. 1.8: Collection locations should prominently display advice on the process for removing private or confidential data. 1.9 Waste that is disposed of to landfill shall be disposed of at a waste facility that is licensed to accept the waste.
	Australian Privacy Principles: the framework support protection of privacy as required in the Privacy Act 1988	Employees health and safety standards.	PP 11 Security of Personal Information:

4 Decision Tree

Determining data disposal requirements

1 **The device is owned entirely by my entity no other parties have interest in the data or the device**

No engage other parties and obtain their approval for destruction

Yes proceed to next step

2 **The data on the device has been assessed and all of it has been approved for destruction and I have considered legal requirements to hold onto this data under the National Archives Act 1983, Privacy Act 1988 and other relevant legislation such as Crimes Act, TSSR and have sought legal advice as to whether the data can be destroyed**

No obtain legal advice on your requirements to retain or record certain types of data

Yes proceed to next step

3 **Assess the classification of the data using an internal label or classification scheme and choose the corresponding disposal**

Public/unofficial (is every data type on this device already publicly available and there is no sensitive personal or organisational information on this device?)

- Disposal process: While publicly available data may not have a cyber related risk, reputational risk exists if identifying data remains on a device which is not responsibly disposed of. Further, as it is highly unlikely that an it device would only contain publicly available information and no sensitive personal or organisational information it is recommended to treat as internal/unofficial.
- Record of sanitisation or destruction for every data bearing point/media to be maintained (noting there are many more points than just the hard drive or solid state drive).

Internal non-sensitive/official

- Disposal process: Sanitisation and destruction allowed as per below.

  Disposal partner: sanitisation and destruction according to the ism by a naid certified (aust regime) partner

  Logistics: secure logistics and/or locked vessels and/or police cleared personnel

  Personnel: police cleared or agsva baseline
- Record of disposal added to files

Confidential commercial sensitive /official sensitive

- Disposal process: Sanitisation and destruction allowed as per below.

  Disposal partner: sanitisation and destruction according to the ism by a NAID certified (aust regime) partner with PSPF endorsement (level 1 official sensitive)

  Logistics: secure logistics and/or locked vessels with tamper evident seals and/or agsva baseline cleared personnel

  Personnel: AGSVA baseline
- Record of sanitisation or destruction for every data bearing point/media to be maintained (noting there are many more points than just the hard drive or solid state drive).

Commercial sensitive restricted/protected

- Disposal process: Sanitisation and destruction allowed as per below.

  Disposal partner: sanitisation and destruction according to the ism by a NAID certified (aust regime) partner with PSPF endorsement (level 1 official sensitive or level 2 secret/top secret depending on data type and organisation type)

  Logistics: secure logistics and/or locked vessels with tamper evident seals and/or agsva baseline cleared personnel

  Personnel: AGSVA baseline or nv1 depending on data type and organisation type.
- Record of sanitisation or destruction for every data bearing point/media to be maintained (noting there are many more points than just the hard drive or solid state drive).

Highly sensitive/secret

- Disposal process: No sanitisation allowed (other than prior to also completing destruction) and destruction as per below.

  Disposal partner: no sanitisation allowed and destruction according to the ism by a NAID certified (aust regime) partner with PSPF endorsement (level 2 secret/top secret)

  Logistics: secure logistics and/or locked vessels with tamper evident seals and/or agsva nv1 or nv2 cleared personnel

  Personnel: AGSVA nv1 or nv2 depending on data type and organisation type.
- Record of destruction for every data bearing point/media to be maintained (noting there are many more points than just the hard drive or solid state drive).

Extremely sensitive/top secret

- Disposal process: No sanitisation allowed (other than prior to also completing destruction) and destruction as per below.

  Disposal partner: not to be outsourced without data owner supervision and nv2 personnel – contact a naid certified (aust regime) partner with pspf endorsement (level 2 secret/top secret) for advice.

  Logistics: secure logistics and locked vessels with tamper evident seals and agsva nv2 cleared personnel

  Personnel: AGSVA nv2 and data owner supervision.
- Record of destruction for every data bearing point/media to be maintained (noting there are many more points than just the hard drive or solid state drive).

5 Resources

1. 2023-2030 Australian Cyber Security Strategy: a nationally coordinated initiative that supports the Australian Government's goal of making Australia the most cyber-secure nation in the world by 2030.

2. AS/NZS 5377: a Joint Australian/New Zealand standard that provides guidance and specifies requirements for the safe and environmentally responsible collection, storage, transport, and treatment of end-of-life electrical and electronic equipment.

3. Australian Energy Sector Cyber Security Framework (AESCSF): an initiative developed by the Australian Energy Market Operator (AEMO), industry and the Australian government. The AESCSF program offers a tool to assess and improve cybersecurity maturity across Australia's energy sector.

4. Australian Privacy Principle (APP): the cornerstone of the privacy protection in the Privacy Act of 1988. The APP is a law-based principle that encompasses 13 guidelines to regulate personal information handling, and a breach of these principles can lead to regulatory action and penalties.

5. Australian Signals Directorate (ASD): the ASD holds a pivotal role within Australia's national security community, undertaking a comprehensive range of modern signals intelligence and security operations that encompass cybersecurity, intelligence, and offensive measures.

6. Essential 8: the multi-faceted tool developed by the ACSC, formulated primarily for safeguarding Microsoft Windows-based internet-connected networks.

7. Information Security Manual (ISM): established by the Australian Cyber Security Centre (ACSC), the ISM provides essential cybersecurity guidelines for organisations to safeguard their systems and data from potential cyber threats. These guidelines cover topics on governance, physical security, personnel security, and information and communications technology security.

8. International Organisation for Standardisation (ISO) 27001: an internationally recognised standard that outlines a systematic approach for organisations to manage and protect their information assets through a robust information security management system (ISMS). It defines the standards for risk assessment, security control implementation and continuous improvement, guaranteeing that organisations preserve the confidentiality, integrity, and availability of their information.

9. National Association for Information Destruction AAA (NAID AAA): NAID is the independent standards setting body for the information destruction industry. NAID's defined criteria within the AAA certification framework certifies companies for the destruction of official information in accordance with the PSPF, through a comprehensive scheduled and unannounced audit program.

10. National Institute of Standards and Technology Cybersecurity Framework (NIST CSF): the NIST CSF emphasises proactive cybersecurity strategy that helps organisations manage and minimise cybersecurity risks. It offers a comprehensive approach to identify, protect, detect, and respond to and recover from cyber threats.

11. Notifiable Data Breaches (NDB) scheme: mandated by the Australian government for organisations and agencies under the Privacy Act 1988, the NDB scheme outlines the specific steps an organisation should take when a breach occurs. It stipulates that these entities must inform the Office of the Australian Information Commissioner (OAIC) and the affected individuals about data breaches that may cause serious harm to individuals whose personal data is compromised.

12. Office of the Australian Information Commissioner (OAIC): the independent regulator for privacy issues and freedom of information. The OAIC manages notifiable data breach reporting and produces several guidance documents of information security, privacy and breach response.

13. Privacy Act 1988 (Cth): the Commonwealth privacy legislation that sets minimum standards to regulate the management of personal information by Australian government agencies, ensuring transparency, accountability, and fairness in handling personal data. The Privacy Act incorporates the 13 Australian Privacy Principles (APPs) alongside enforcement mechanisms to guide the proper handling of personal information and ensure compliance.

14. Protective Security Framework (PSPF): the PSPF is renowned for supporting Australian Government entities in safeguarding their personnel, information, and assets both domestically and internationally. It outlines the government's protective security policies and assists entities in efficiently implementing these policies across security governance, information security, personnel security, and physical security outcomes.

15. Security of Critical Infrastructure (SOCI) Act 2018: amended in 2021, the SOCI Act is a commitment by the Australian government to protect essential services Australians rely on and uplift the resilience and security of Australia's critical infrastructure across various 11 different sectors.

16. Security of Critical Infrastructure Act 2018: this Act focuses on establishing a comprehensive framework for managing national security risks associated with critical infrastructure. It aims to facilitate cooperation between government, regulators, infrastructure owners and operators to identify and address critical infrastructure risks.

17. The Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Enforcement Act): an amendment that increases penalties under the Privacy Act 1988. This bill gives the Australian information Commissioner greater enforcement authority and facilitates greater information sharing powers between the Commissioner and the Australian Communications and Media Authority (ACMA).

WV Technologies is a multi-award winning Indigenous Social Enterprise which provides fully compliant IT Disposals and e-Waste recycling to organisations of all sizes and at all security levels across Australia.

WV Technologies holds all recycling and security certifications with NAID AAA Certification and PSPF Endorsements to **top secret** along with a range of other certifications.

Working with WV Technologies will achieve environmental impact and social impact for Indigenous people.

www.wvtech.com.au
services@wvtech.com.au

Contributing Authors

Jamie Miller

Co-Founder
WV Technologies

Kurt Gruber

Co-Founder
WV Technologies

Robert Di Pietro

Partner
Cybersecurity &
Privacy Lead

Explore more
pwc.com.au

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au

D0681430