**guidance for developing an r2v3 data sanitization plan**

**Version: 1**

***Guidance is intended to offer further explanation of the requirements in the R2 Standard along with examples and audit recommendations. However, this document is not auditable and cannot be cited in relation to any nonconformances. The explanations are intended to prevent misinterpretation of the R2 Standard, not to add to, subtract from, or modify the R2 Standard. The examples cited may not be the only way to fulfill a requirement of the standard.***

Although reasonable care was taken in the preparation of this document, SERI and any other party involved in the creation of the document HEREBY STATE that the document is provided without warranty, either expressed or implied, of accuracy or fitness for purpose, AND HEREBY DISCLAIM any liability, direct or indirect, for damages or loss relating to the use of this document.

When developing your Data Sanitization Plan, consider each of the steps and key questions below to help guide you through the process and ensure the development of a comprehensive plan. Note that each section relates to a specific requirement in the R2v3 Standard, but the requirements below are not listed in the same order as they appear in the Standard, as they have been sequenced in a manner to better facilitate your plan development.

For each section, note in detail how the questions and examples specifically apply to your facility’s operations. Indicate any associated resources required to implement the R2 requirement or demonstrate conformance with it or the plan. Resources may include procedures, work instructions, checklists and forms (existing or to be developed) that support the data security and sanitization processes. The sample notes provided demonstrate how your responses can be captured, but these are examples only and must be expanded upon and revised as applicable to your facility’s operations. Your responses in each of these sections will provide the initial framework for your Data Sanitization Plan, so provide as much detail as possible. And, keep in mind that the plan will periodically need to be reviewed and revised, particularly where there are any changes in processes, devices managed or other applicable data requirements.

| **Step #1: Identify the types of data storage devices and the related data managed by your facility** | | |
| --- | --- | --- |
| **Reference** | **Key Questions** | **Notes** |
| 7.(a)(1)(B) | ***Data*** is defined in R2v3 as “*the private, personally identifiable, confidential, licensed or proprietary information contained on an electronic device or memory component*.”  All data devices and media require secure management and sanitization.  Considering all types of electronic devices, components and media managed by your facility, what specific types of devices are capable of storing data?  For example, in addition to laptops, desktops and servers that are commonly recognized as data devices, does your facility accept SSDs, wearable electronics, tablets, smart TVs, mobile devices, or other items that can also store data?  Consult the [*Examples of Common Characteristics of Select Electronic Devices*](https://sustainableelectronics.org/wp-content/uploads/Common-Device-Characteristics-21.06.18.pdf) and NIST Guidelines for Media Sanitization (Appendix A), for examples of various types of data devices. | *Note each type of data device/media managed by your facility:*   * *e.g. Mobile phones* * *Tablets* * *SD cards* * *SIM cards* * *etc.* |
| 7.(a)(1)(C) | For each type of data device managed, what types of data does it potentially contain that requires sanitization?  Consider user files and accounts; operating systems; licensed software; user logs; etc. and list all data types by device. Understanding the types of devices and data stored will help to identify what requires sanitization. | *List all data devices managed and the corresponding types of data to be sanitized:*   |  |  | | --- | --- | | ***Device*** | ***Data*** | | *e.g. Mobile phone* | * *User files* * *User accounts* * *Licensed software* * *etc.* | |
| 7.(a)(1)(D) | ***General information*** is defined in R2v3 as “*publicly available information or information that is provided with the original electronic equipment from the manufacturer.”*  General information does not require sanitization under R2v3.  For each type of data device managed, what types of general information does it contain that does not require sanitization?  For example, general information may include drivers and firmware; open source software or operating systems; electronic user manuals; etc. | *List all data devices managed and the corresponding types of general information that does not require sanitization:*   |  |  | | --- | --- | | ***Device*** | ***General Info*** | | *e.g. Desktop computer* | * *Firmware* * *Open source software* * *Electronic user manuals* * *etc.* | |
| 7.(a)(1)(E) | In some cases, devices may rely on remote services for storing and accessing data through connected user accounts.  What types of network services and other connected accounts are there that require removal from the device?  Consider cloud-based accounts and back up storage drives; as well as paired devices. | *List all data devices managed and the corresponding network or connected user accounts that require removal:*   |  |  | | --- | --- | | ***Device*** | ***Accounts*** | | *e.g. Tablet* | * *System accounts - Google; iOS; MS…* * *Online storage – Box, DropBox…* * *Media accounts – Netflix; Spotify…* * *etc.* | |

| **Step #2: Define all data security and sanitization requirements** | | |
| --- | --- | --- |
| **Reference** | **Key Questions** | **Notes** |
| 7.(a)(1)(G) | In addition to the R2 requirements, are there specific legal, supplier or other requirements for data security or sanitization that also need to be addressed?  Does your facility’s legal compliance plan clearly identify data sanitization requirements such as data breach and privacy regulations?  Are there additional contractual requirements from suppliers related to data security and sanitization? | *List any other data security and/or sanitization requirements:*   |  |  | | --- | --- | | ***Legal*** | ***Applicability*** | | * *e.g. GDPR* * *CCPA* * *HIPAA* * *etc.* | * *e.g. Documented data assessments & audits* * *Defined data access & authorizations* * *Reporting requirements* * *etc.* | | ***Supplier*** | ***Applicability*** | | * *e.g. OEM* * *Retailer* * *PRO* * *etc.* | * *e.g. Method of sanitization* * *Time-frame for sanitization* * *Method of notification of sanitization* * *etc.* | |
| 7.(a)(1)(H) | For each of the additional legal, supplier or other requirements identified, is there a clear link to where it is addressed in your facility’s written policies and procedures?  For instance, if there are requirements for an increased level of security, or a particular method of sanitization, are the requirements clearly identified and defined in your facility’s written documentation? | *Identify where each of the additional security and sanitization requirements is addressed in the processes and procedures to ensure conformance.* |
| 7.(a)(1)(J) | Have specific time-frames for performing sanitization been identified?  Consider whether there are legal or supplier requirements that stipulate the maximum period from time of receipt until sanitization.  Also consider the level of sensitivity of data managed and the risks associated with a potential data breach, when establishing the sanitization period. | * *Clearly identify the required time-frame for completing sanitization from the point of receipt of a data device.* * *Define the process used to track the devices and ensure sanitization within the defined time-frame.* |
| 7.(a)(1)(F) | Has a contractual agreement been developed and put in place with any customer that requires their data not be sanitized? | * *Define the specific conditions where data will not be sanitized, such as when a device is repaired and returned to the user.* * *Ensure a process is in place to contractually note and track each customer’s request not to sanitize their device.* |

| **Step #3: Establish the data sanitization processes and procedures** | | |
| --- | --- | --- |
| **Reference** | **Key Questions** | **Notes** |
| 7.(a)(1)(I) | Considering all types of data devices managed and the applicable requirements for sanitization, have defined methods of sanitization been identified for each type of device and media?  Do the defined methods of sanitization align with one of the options for sanitization as defined in Core 7.(c)(2)?  For devices that are logically sanitized, do the processes outline the approved method of sanitization if the logical sanitization is not successful? | *Identify the approved method of sanitization for each data device managed:*   |  |  | | --- | --- | | ***Device*** | ***Method of Sanitization*** | | *e.g. Mobile phone* | * *Logical software sanitization (Appendix B)*   *or*   * *Shred and reduce chips to fragments (Appendix B)* |      |  |  | | --- | --- | | ***Device*** | ***Method of Sanitization*** | | *e.g. HDD* | * *Shred (Core 7 / NIST 800-88)* | |
| 7.(a)(1)(I) | For data sanitization activities that are performed internally, are there data sanitization procedures or work instructions to define the approved process and steps to sanitize each type of device? | *Cleary define the process and procedure for handling and sanitizing each type of device.* |
| 7.(a)(1)(K) | Are DSVs required to perform any of the physical or logical sanitization?  If so, have the DSVs been qualified in accordance with Appendix A (7) or (8)?  Is there evidence that the DSV conforms with the requirements of the Data Sanitization Plan? | * *Clearly identify all DSVs responsible for data sanitization in the downstream recycling chain flowchart as per Core 8.(a)(3);* * *Maintain adequate evidence of qualification of each DSV under Appendix A; and* * *Maintain evidence of conformance with the Data Sanitization Plan.* |
| 7.(a)(1)(L) | Has the intended outcome or results of the sanitization process been clearly defined so the effectiveness of the process can be verified?  Has the verification process been defined?  Are records maintained to demonstrate effective sanitization? | *For each data device, identify the approved method of sanitization as well as the method for verifying success of the process, and the records used to demonstrate the sanitization and verification activities:*   |  |  |  |  | | --- | --- | --- | --- | | ***Device*** | ***Method of Sanitization*** | ***Verification*** | ***Records*** | | *e.g. HDD* | *38mm (1½”) Shred* | * *Visual inspection of shred* * *Mass balance of processed volumes* | *Process logs and mass balance tracking* | |

| **Step #4: Establish security controls** | | |
| --- | --- | --- |
| **Reference** | **Key Questions** | **Notes** |
| 7.(a)(1)(A) | Considering the types of data devices managed, the level of sensitivity of the associated data, and any other specific data security requirements, have appropriate security controls been developed to protect the devices and data?  Have dedicated secured areas for data sanitization activities been established with restricted access?  Consider whether to secure individual areas for sanitization activities or the entire facility.  Also consider the types of security controls required, such as:   * Physical controls, including dedicated locked rooms or partitioned areas with physical barriers; locks and/or monitored electronic access control to restricted areas; security alarms and monitoring systems; etc. * Process controls, including security training & awareness; access authorizations; security monitoring; material handling procedures; etc. | *Clearly demonstrate where all security controls of 7.(b) are addressed.*  *Facility Security Controls:*   * *e.g. Secured entry with key FOB access* * *Security cameras and monitoring system* * *Labeled and clearly identifiable secured areas with restricted access* * *etc.*   *Sanitization Area Controls:*   * *e.g. Secured entry with key FOB access and limited access authorizations* * *etc.*   *Process Controls:*   * *e.g. Worker data security training* * *Receiving and storage procedures* * *etc.* |
| 7.(a)(1)(M) | Is there a process in place for defining and providing security authorizations for anybody accessing areas with data containing equipment and components?  Does the process address workers, visitors and others that may be present in your facility such as contractors?  Are there processes in place for monitoring those that access the secured data areas? | *Clearly identify:*   * *Levels of security authorizations;* * *How authorizations are granted;* * *How data secured areas are identified and access restrictions communicated; and* * *How access to data secure areas is monitored and enforced.* |
| 7.(a)(2) | Has a data security policy been documented to identify the responsibilities, authorities and restrictions related to data security and sanitization?  Has the Data Protection Representative been identified?  Have incident reporting and responses procedures been defined? | *Clearly identify:*   * *Who the Data Protection Representative is;* * *All authorities, responsibilities and restrictions related to data;* * *Requirements for reporting known or suspected data breaches;* * *Training and confidentiality requirements for individuals handling data devices; and* * *Processes for investigating and responding to data incidents.* |

| **Step #5: Where applicable, develop additional data controls related to Appendix B processes** | | |
| --- | --- | --- |
| **Reference** | **Key Questions** | **Notes** |
| B (1)(a) | Have methods been developed to identify and distinguish sanitized devices from those containing data? | *Clearly identify any device tracking, labelling, separate physical storage areas and other controls used to separate and distinguish sanitized devices.* |
| B (1)(b) | Have quality controls been defined to assess and verify the effectiveness of the data sanitization processes?  Are quality controls implemented on an ongoing basis?  Is there a process in place to notify suppliers of any processing discrepancies?  Is there an alternate process to manage devices where data sanitization cannot be verified? | *Define the quality controls used to verify the sanitization processes, demonstrating that:*   * *All data devices were processed as planned;* * *Output from the sanitization process is consistent with the planned method; and* * *Quantities processed match quantities received.*   *Define the corrective action process for responding to any issues identified in the sanitization process.* |
| B (1)(c) | Have activities been defined for monitoring the aspects of the Data Sanitization Plan to ensure they are implemented as planned and effective? | *Define the activities that are used to oversee the implementation of the data sanitization plan such as:*   * *Performance tracking;* * *Audits and inspections;* * *Tracking and analysis of customer or other external feedback;* * *Incident investigations; and* * *Corrective action follow-up.* |
| B (1)(d) | Have data sanitization competency requirements been defined? | *Clearly identify all competency requirements related to:*   * *Performing each data sanitization process; and* * *Verifying the data sanitization activities.* |

| **Step #6: Develop processes for training on and validating the security and sanitization controls** | | |
| --- | --- | --- |
| **Reference** | **Key Questions** | **Notes** |
| 7.(a)(3) | Have all workers been trained on the applicable data security and sanitization processes and controls?  Is regular upgrade or refresher training planned and conducted?  How is the competency of responsible individuals verified? | *Clearly identify:*   * *Approved data security and sanitization training programs;* * *Individuals/roles requiring specific data training;* * *Plans and schedules for conducting regular refresher training; and* * *Methods for verifying and records to demonstrate competency.* |
| 7.(c)(3) | Has an internal data security and sanitization audit process been developed?  Are trained, competent and independent auditors assigned to and responsible for conducting the data audits?  Ensure the audit process assesses conformance with:   * R2v3 requirements * Legal requirements * Internal processes and procedures * Customer, supplier and other requirements | *Clearly identify:*   * *The data security and sanitization audit process and criteria;* * *Audit schedule;* * *Responsibilities, competency and independence of auditors; and* * *Process for tracking the results of the audit process including any follow up actions as a result of issues identified.* |