Secure Digital Media Sanitization Standard

Cybersecurity Division

Technology and Innovation

Version: 2.0

Approved by: Assistant Deputy Minister (ADM) & Chief Information Security Officer, Cybersecurity Division, Technology, and Innovation	**Owner:** Assistant Deputy Minister (ADM) & Chief Information Security Officer, Cybersecurity Division, Technology, and Innovation	
Approval date: April 3, 2023	**Review date:** November 23, 2022	**Next review date:** November 2023
Contact: Cybersecurity Division, cybersecurity@gov.ab.ca	**Policy Instrument type:** Standard	

Contents

Standard Statement

The Secure Digital Media Sanitization standard defines secure methods for sanitization (erasure) of electronic media including but not limited to magnetic, optical, and flash media, within the Government of Alberta (GoA).
Information Security Management Directives (ISMD) require that digital media be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media. This standard supports Information Security Management Directives (ISMD) section 2.3.1, 2.3.8, and 2.3.9.

Authority

This standard derives its authority from Information Management and Technology (IMT) Policy and IMT policy definition.

Scope

This standard applies to all Ministries within the GoA (or their agent) for the following:

1. The secure disposal of digital media.
2. The reassignment of hardware and/or media to another person internal or external to the GoA.

This standard applies to all GoA digital media, regardless of its data classification, the media upon which it is stored, and whether it is on premise or in the cloud.

This standard does not waive any requirement for records disposition under an approved records retention and disposition schedule. The standard specification is in effect once the decision is made to securely destroy media that contains or did contain GoA information.

Standard Description

This standard provides guidance on appropriate methods for protection of GoA information and data using a secure digital media sanitization process. The methods used to dispose of GoA data depends on the classification of the data. Media sanitization protects the confidentiality of sensitive information that is stored on any digital medium, hard disks, Solid State Drives (SSD), magnetic tape, and all other electronic storage mediums. Secure and effective disposal is required for GoA digital media that is no longer required, end of life, or damaged beyond repair. Without secure digital media sanitization, unauthorized individuals could reconstruct data and gain access to sensitive information.

Standard Specification

This standard defines four (4) methods for securely sanitizing data stored on GoA digital media. Note that disposal of media is not supported in the GoA for any information classification. The methods are described in the following table:

Method	NIST 800-88 Description
Disposal	Disposal is the most basic form of sanitization, where media is tossed out with no special disposition given to them. For media containing GoA Data, **disposal is NOT an acceptable** sanitization method.
Clearing	Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. Overwriting is an acceptable method for clearing **public classified data** that was stored on media.
Purging	Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging **protected A and B classified data** that was stored on media. Note: Degaussing **is not** an appropriate method of purging data from flash media.
Destroying	Destruction of media is the ultimate form of sanitization. After the storage medium is destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. For media containing GoA **protected C classified data** is recommended method.
Crypto-Shredding	This method involves encrypting the data with a strong encryption engine and then taking the keys generated in that process, encrypting them with a different encryption engine, and destroying the resulting keys of the second round of encryption.

Method	NIST 800-88 Description
(**Cryptographic Erasure) – for data in Cloud**	

Verification of Secure Media Sanitization Standard Specification

Verification of the sanitization and disposal process is an essential step in assuring the storage medium was properly sanitized. A representative sampling of should be tested after sanitization has been completed.

Record Keeping for Secure Media Sanitization Standard

The GoA must maintain records of its sanitization activities. The information to be recorded includes, but is not limited to the following:

- What media was sanitized,
- When the media was sanitized,
- Data classification
- Number of media sanitized,
- How it was sanitized,
- Whether verification was performed, and
- The final disposition of the media.

In cases where information system media is located offsite and managed by a third party, such as cloud providers Software or Platform as a Service (SaaS, PaaS), the Service Level Agreement (SLA) requires verification forms be provided to the GoA after sanitization is completed.

Definitions

- **Crypto-Shredding:** A method of sanitization in which the media encryption key (MEK) for the encrypted Target Data is sanitized, making recovery of the decrypted Target Data infeasible.
- **Degausser:** A device that can generate a magnetic field. Used to remove the magnetism from a data storage device, destroying the data housed on it.
- **Media Sanitization:** The general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

Roles and Responsibilities

Information Controllers:

- ensure that maintenance agreements and/or contracts are in place that protect the confidentiality of GoA information, and the media upon which it is stored. The degree of protection provided must be commensurate with the risk of disclosure.
- are responsible for ensuring that the information assets they are responsible for is classified, and that the users and administrators of the information are aware of its confidentiality and the basic requirements for media sanitization.

Information Custodians:

- are responsible for ensuring that sanitization efforts comply with this standard; and
- are responsible for the process, procedures and tools used to destroy digital media.

Data Privacy and Innovation - Content Management:

- advises Information Controllers and Custodians on retention requirements that must be met to ensure that sanitization of media will not destroy records that should be preserved.

Compliance

Consequences of non-compliance with this standard could result in damage to Government of Alberta's reputation, exposure of Albertans to harm and/or incurrence of unnecessary costs. Depending on the severity of non-compliance:

- either informal or formal requests and/or follow-ups may be made the Data, Privacy and Innovation Division, Corporate Internal Audit Services, Cybersecurity Division, Office of the Auditor General, Office of the Information Privacy Commissioner, and/or Public Service Commission, and
- legislated disciplinary action (i.e., *Public Service Act*) may be taken.

The GoA may revise this standard from time to time and will communicate amendments to stakeholders in a timely manner.

References and Supporting Resources

- Information Security Management Directives
- Degausser Evaluated Products List (National Security Agency)
- IT Media Sanitization (Communications Security Establishment)
- Guidelines for Media Sanitization (NIST SP800-88, Rev.1)
- Data and Information Security Classification
- Records Management Regulation
- Cryptographic Erasure
- Content Management Policy