	Georgia Technology Authority	
Title:	**Media Protection and Handling**	
PSG Number:	**SS-08-043**	
Effective Date:	**03/31/2008**	**Review Date: 12/01/2024**
Synopsis:	Establishes physical, logical, and environmental protection requirements for system media	

PURPOSE

Media controls include a variety of measures to provide physical and environmental protection and accountability for removable or mobile media, regardless of its physical form, whether paper or digital, including but not limited to printouts, laptops, PDAs, removable storage devices, etc. Media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software when stored outside the physical or logical security boundaries of the system. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(9) – *State Government, Georgia Technology, General Powers*

O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*

PM-04-001 – *Information Technology Policies, Standards and Guidelines*

PS-08-005 – *Enterprise Information Security Policy*

TERMS and DEFINITIONS

System Media – any form of data or software stored outside the security boundaries of the system such as, but not limited to paper printouts, tapes, diskettes, flash memory drives (USB, jump, thumb), internal hard drives, laptops (undocked), PDAs, CDs, DVDs etc.

STANDARD

Data Owners shall establish procedures and take the following actions to ensure that system media and its contents, whether paper or digital is protected from unauthorized access, disclosure, modification, destruction or loss.

- Media containing sensitive or critical information or requiring special handling shall be appropriately marked or labeled to ensure proper handling and storage.
- Off-site hardware maintenance agreements shall be accompanied by a vendor signed statement of non-disclosure and handled in accordance with the Media Sanitization-Vendor Return standard.
- Where applicable the media shall be removed, sanitized and/or backed-up prior to sending off-site for maintenance.
- Logs, control numbers, or other tracking mechanisms in addition to appropriate physical protection shall be used for media containing information requiring strict access accountability and/or chain-of-custody verification (including media sent off-site for maintenance).
- Where appropriate, cost effective and/or required to meet established security levels, portable media and storage devices shall have access controls and data shall be encrypted.
- Portable media devices shall be securely stored when not in use and protected from physical and environmental hazards.
- Media shall be disposed of or retained in accordance with applicable policies and standards.
- Education and awareness programs shall include guidance on appropriate use, proper protection and handling of media, irrespective of media ownership.
- Data Custodians shall be advised of security requirements and/or data sharing agreements and establish procedures to comply with those requirements.

Use of personally owned media shall not disestablish the applicability of this standard. All media, whether state issued or personally owned, shall be subject to the protection requirements established in this standard as well as the policies and standards governing appropriate use. All media used within State of Georgia workspaces shall be subject to search and seizure if warranted.

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Media Controls (PS-08-026)
Surplus Electronic Media Disposal (SS-08-034)
Media Sanitization – Vendor Return (SS-08-035
Data Security – Electronic Records (SS-08-003)
Privacy in the Workplace (SS-12-001)

Non-State Technology and Computing Devices (SS-02-002)

REFERENCES

NIST SP 800-12 (chapter 14) Introduction to Computer Security NIST Handbook