**Media Protection Policy**

# Purpose

This Policy describes requirements for protecting restricted SLEDS Information on media, including paper, external drives, workstations, and digital storage.

# Scope

This Policy applies to the SLEDS Environment, SLEDS Information, Participating Entities, and other parties authorized or responsible for carrying out SLEDS Policies.

# Applicable Standards and Regulations

* Federal Education Rights and Privacy Act (FERPA), [§20 U.S.C. § 1232g; 34 CFR Part 99](https://www.law.cornell.edu/uscode/text/20/1232g).
* [Unemployment Insurance Program Letter, No. 14-17](https://wdr.doleta.gov/directives/attach/UIPL/UIPL_14-17.pdf) (dated March 23, 2017) regarding States' Responsibilities for Internal Security in the UI Program
* Federal and State privacy and security rules and regulations governing SLEDS Information including, but not limited to e-CFR [§§ 99.1 - 99.67](https://www.ecfr.gov/cgi-bin/text-idx?SID=21a8457a1789d118dcdce055ca195995&mc=true&tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl)
* [NIST (SP) 800-171, Rev. 2](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf) requirements and corresponding International Organization for Standardization/ International Electrotechnical Commission (ISO/ IEC) 27001 Security Controls
* State of Wyoming Information Technology Policies and Standards, including but not limited to:
	+ [General Policies and Standards](http://ets.wyo.gov/resources/policies-and-standards/10000-general)
	+ [Security and Privacy Policies and Standards](http://ets.wyo.gov/resources/policies-and-standards/09000-security)
	+ [Information Management and Control, Document Management Policies and Standards](http://ets.wyo.gov/resources/policies-and-standards/08000-documents)
	+ [Facilities, Logistics, Natural Resources and Environmental Policies and Standards](http://ets.wyo.gov/resources/policies-and-standards/04000-facilities)
	+ [Plans and Operations; Research and Development Policies](http://ets.wyo.gov/resources/policies-and-standards/03000-plans)
	+ [Manpower and Personnel Policies and Standards](http://ets.wyo.gov/resources/policies-and-standards)

# Policy Statements

The State of Wyoming’s technology policies and standards are the minimum control requirements. More restrictive controls shall apply to the SLEDS Environment as provided in this Policy.

| 1 | Participating Entities shall remove SLEDS Data from electronic devices and electronic media under their control or ownership in alignment with Wyoming State IT Policy [09400-P164 Policy Preparation of Electronic Devices and Media for Disposal](https://docs.google.com/document/d/1DvrpDED4WwDdtTdjRPyYVLtqwyVJI5m3HGdp5jcWJSs/edit). |
| --- | --- |
| 2 | Participating Entities shall manage their logical and physical access controls of the hardware and software that processes SLEDS data in a meaningful way in alignment with the [SLEDS Access Control Policy](https://docs.google.com/document/d/1yaj5y70bQAtYY7gnaXBIZFh0KsGsDBE2nPHRXG0o634/edit?usp=sharing) and the [Access Control Procedure](https://docs.google.com/document/d/1SOnBZ4xKW_2yvp4M2KBZVUyfAKILw07HWo8k7p4js-A/edit). This includes applications, peripherals, removable media, other components and could be one computer or a network of computers, as stated in the Wyoming State IT Policy. |
| 3 |  WCCC IT staff shall document and confirm proper authorization controls for restricted information, including Personally Identifiable Information (PII). This policy will be enforced to ensure proper access controls in alignment with [SLEDS Identification and Authentication Policy](https://docs.google.com/document/d/1aURaTkelS-Uqkibtu8Fmg247WfYhdkEUlXbyL50tqWk/edit?usp=sharing), the [SLEDS Access Control Policy](https://docs.google.com/document/d/1yaj5y70bQAtYY7gnaXBIZFh0KsGsDBE2nPHRXG0o634/edit?usp=sharing), and the [Access Control Procedure](https://docs.google.com/document/d/1SOnBZ4xKW_2yvp4M2KBZVUyfAKILw07HWo8k7p4js-A/edit). |
| 4 | All electronic devices and media storing SLEDS Information will be erased, encrypted, sanitized or destroyed in alignment with the [SLEDS Data Destruction Policy](https://docs.google.com/document/d/1t8o361rOCRJZFSDJrFfIX2ctaYKWlayA2_laH5Y4g-g/edit) and the [Data Destruction Procedure](https://docs.google.com/document/d/11Ki-peHjYJlwszvmESqaCQWRQsXudmfY8pWMJGSbYk4/edit). |
| 5 | All workstations networked to the SLEDS Environment shall maintain current Windows and software updates. All WCCC workstations shall employ drive-level encryption. |
| 6 | No USB or other removable devices shall be utilized or allowed to store SLEDS Information. |
| 7 | WCCC may conduct scans to enforce controls restricting the use of USB drives or other removable devices. |

# Additional Information

Additional and supporting information can be found using the following resources:

* [SLEDS Glossary of Defined Terms](https://docs.google.com/document/d/1_Im9iujOTJ_kIkbDNMfBABWkPYysFLustW4ia0mLoHs/edit)
* [SLEDS Policy and Procedure Inventory](https://docs.google.com/spreadsheets/d/1_rOCVJux4kfzYjs6963l2MYuLN3iSF0hYZH01BmvYbU/edit#gid=1266995384)
* [SLEDS Data Research Request Process](https://docs.google.com/document/d/1JuZsHks1hhexjJwbSd4gwmUvMYGzYoTha6E1BJkYTZI/edit)
* [U.S. Department of Education FERPA Guidance](https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
* [PTAC Guidance on Integrated Data Systems](https://studentprivacy.ed.gov/resources/integrated-data-systems-and-student-privacy)
* [PTAC Summary of FERPA Exceptions](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20Exceptions_HANDOUT_portrait.pdf)

For questions or concerns related to this Policy, please contact the Wyoming Community College Commission Chief Technology Officer (CTO) at (307) 777-7763.

###

## Revision History

| **Revision #** | **Revision Date** | **Summary of Changes** | **Changes marked** |
| --- | --- | --- | --- |
| 1.0 |  | Approved Policy | N/A |
| 1.1 | 11/17/2020 | Included cross-references to additional policies and procedures. | Yes in Red font and underlined. |
| 1.2 | 11/24/2020 | Accepted changes from 1.1 and rebaselined. | N/A |
| 1.3 | 6/21/2021 | Updated policy references to revised [NIST (SP) 800-171, Rev. 2](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf) standard | N/A |

##  Approvals

This policy requires the following approvals:

| **Name**  | **Date Approved** |
| --- | --- |
| Security Subcommittee | v1.2: 11/24/1010 |
| Data Governance Committee | v1.2: N/A, Approval not needed since only minor changes incorporated and no changes to the policy itself were made. |