**Access Control Policy**

# Purpose

This Policy defines the circumstances where identification and authentication (I&A) controls such as limiting access and using user IDs and passwords to SLEDS Information. It addresses access control to the SLEDS Environment.

# 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 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)
	+ [09400-P170 Policy User Access Management](https://docs.google.com/document/d/1HCc-7_pc917TzgJr_RHLqvsDw1cEgLqViOEWHZ1JisI/edit)
	+ [09400-S170 Password Standards](https://drive.google.com/file/d/0B_YE8dWRQWQAY0hKTm5yNzkwTEU/view)
	+ [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)
* SLEDS High Availability Data MOU (HADS)

# 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 | Logical and physical access controls for the SLEDS Environment shall align with Wyoming State IT Policies: [09400-P173 Policy Access Controls on IT Resources](https://docs.google.com/document/d/1xzbGwaLuGBXsCszyqfgRkUp8PBzDamCquErEhI1EHzI/edit)[09400-P170 Policy User Access Management](https://docs.google.com/document/d/1HCc-7_pc917TzgJr_RHLqvsDw1cEgLqViOEWHZ1JisI/edit)[09400-S170 Password Standards](https://drive.google.com/file/d/0B_YE8dWRQWQAY0hKTm5yNzkwTEU/view) |
| --- | --- |
| 2 | SLEDS Participating Entities shall maintain logical access controls for Personally Identifiable Information (PII) as it relates to a Participating Entity’s data or any integrated data within the SLEDS Environment. |
| 3 | Whenever logical access controls are needed, at least one technical component must ask for the requestor’s identification (UserID) and successfully validate the authentication (password) before the requested information or service can be accessed. Any SLEDS components requiring authentication or use of Transport Layer Security (TLS) Certificates web sites and web applications shall follow the requirements set out in State Policy [09300-P010 Web Transport Layer Security (TLS) Certificate Use](https://docs.google.com/document/d/1f6l_jpdKVNNAwX1kddwxRzGkUTqZ2mJB81fH7-faVvE/edit). |
| 4 | Systems that request UserIDs and passwords shall mask, suppress, or otherwise obscure the display and printing of passwords so that unauthorized parties will not be able to observe or subsequently recover them. |
| 5 | If any part of the login sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the login process was incorrect. |
| 6 | The number of unsuccessful logon attempts shall be limited. Users that are unsuccessful at logging on within the prescribed number of tries shall be locked out for a prescribed period of time. |
| 7 | Access to system utilities shall be limited to users and administrators with an approved need to run or use those utilities. Other uses of and access to those utilities shall be granted on a temporary basis only after a business requirement for this access has been documented and approved. Unneeded system utilities, options, and/or services shall be removed or disabled. |
| 8 | Warning banners shall be displayed during initiation of the login process to networks and where appropriate, to other resources prior to requests for UserIDs and passwords in alignment with Wyoming State IT Standard [09400-S173 Security Warning Banner](https://docs.google.com/document/d/1PikTxjDKvKLF-_g6eWjg_fZ12t33tWL8LLXmvUN-c4c/edit). |
| 9 | Screensavers (sometimes called “screen locks”) shall be automatically activated and password protected on terminals after a prescribed period of inactivity in alignment with Wyoming State IT Standard [09400-S176 Automatic Screen Lock](https://docs.google.com/document/d/1zXPgLNHcqsvsIPRgz7YFQcB4_qlG8__WIaRTYkJrCww/edit). |
| 10 | System and database administrators shall configure operating systems and databases to implement and enforce applicable password management requirements. |
| 11 | All users and other entities (applications, systems, etc.) must be uniquely identified to the information system(s) they access and shall only have access to resources for which they have been explicitly authorized. |
| 12 | Direct connections from the Internet to internal, non-public, database systems, even to view data, shall not be allowed. All confidential data shall be encrypted end to end, from server to server, at rest and in transit. This does not include third parties supporting database management or other maintenance, provided they are connecting via a protected path. |
| 13 | Access control devices shall be configured and managed in alignment with the [SLEDS System and Communications Protection Policy.](https://docs.google.com/document/d/1sN874DMvQfPY24hWqvHQ4hiNCSNhvbTXMk5xYC-FH1Q/edit?usp=sharing) |
| 14 | Data shall be encrypted at rest and in transit in alignment with State Policy [09400-P220 Policy Data at Rest and in Transit](https://docs.google.com/document/d/1ONwLqj0jaSvrdlQEA35qzfLK4GdAdGTbsxcn0rOORPk/edit). |

# 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 | N/A | Approved Policy | N/A |
| 1.1 | 9/1/20 | Added references to additional ETS password standards | Red Underline Text |
| 1.2 | 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 |
| 2.1 | 5/11/2022 | Added a reference to the SLEDS High Availability Data MOU.  | Red text |
| 2.2 | 5/11/2022 | Changed “ETS Policy” to “State Policy  | Red Text |

##  Approvals

This policy requires the following approvals:

| **Name**  | **Date Approved** |
| --- | --- |
| Security Subcommittee | v2.1: 6/21/2022v2.2: 6/21/2022 |
| Data Governance Committee | v2.1: 7/12/2022v2.2: 7/12/2022 |