**Risk Assessment Policy**

# Purpose

This Policy provides baseline requirements for risk assessments of the SLEDS Environment. Risk assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, and sensitive information leakage.

# 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 | Risk assessments shall be periodically performed to identify potential or realized weaknesses as a result of scenarios such as inadvertent misconfiguration, weak authentication, insufficient error handling, and sensitive information leakage. Such assessments should target identification of weaknesses to the confidentiality, integrity, and availability of the information in the SLEDS Environment; and risks to, and availability of, the SLEDS Environment to provide its normal business functions. Such assessments should support and inform the tasks and activities set out in the [SLEDS Security Assessment Policy](https://docs.google.com/document/d/1BKI-CwanardXe8ZTTvForGnENIojigH72OR77Hk4xnI/edit?usp=sharing). |
| --- | --- |
| 2 | An operational program or function shall be established to ensure risk assessments against the SLEDS Environment are performed, as well as performing automated and manual scanning for vulnerabilities in alignment with the [SLEDS Information Systems Integrity Policy](https://docs.google.com/document/d/16B_4-zIHF1G_c2mVy5eBGhfnHxce1aAubM2GbBVCuEw/edit). |
| 3 | Risk assessments should be conducted for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use within the SLEDS Program and/or SLEDS Environment. 1. All risk assessments will be performed by the SLEDS Security Team or delegate(s).
2. All risk assessment findings are considered confidential and are to be distributed to individuals on a “need to know” basis. Risk assessment results shall be documented in a risk assessment report, a security compliance report, or in some other format to be provided to the Information Resource Owner and others who have a role and responsibility in SLEDS risk assessments.
3. Distribution of any findings is strictly prohibited unless approved by the State Chief Information Officer.
4. Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.
5. The assessment of risks should include the likelihood and magnitude of harm from an event that could compromise the security policies and compliance of the technologies in the SLEDS Environment.
6. Through the SLEDS Governance Structure, Participating Entities should be informed about any known risks and consulted prior to placing new system components into production.
7. The risk assessment shall be updated upon request of the SLEDS Data Governance Committee as recommended by the SLEDS Security Team, and whenever there are significant changes to the SLEDS Environment including the identification of new threats and vulnerabilities.
 |
| 4 | SLEDS web application assessments shall be performed in alignment with Wyoming State IT Policy [03500-P018 Web Application Security](https://docs.google.com/document/d/1ekB0iNcqyNK_2MHYVsf_fjepzCq8fub6GbIZ9JxE8BQ/edit). Web applications are subject to assessment based on the following criteria:1. New or Major Application Release – Will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
2. Third Party or Acquired Web Application – Will be subject to a full assessment after which it will be bound to policy requirements.
3. Point or Minor Releases – Will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
4. Patch Releases – Will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
5. Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the State Chief Information Officer or their delegate.
 |
| 5 | All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater. 1. High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
2. Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
3. Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.
 |
| 6 | The following assessment levels shall be established: 1. Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk.
2. Quick – A quick assessment will typically consist of an automated scan of an application for at least the OWASP Top Ten web application security risks.
3. Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.
 |
| 7 | Risk assessments shall be performed in connection with networking and/or communication resources being connected to the SLEDS Environment to form networks in alignment with the [SLEDS System and Communications Protection Policy](https://docs.google.com/document/d/1OQOdnpLYYEfP6Zm56_ZEd1lPDzH5hcBQmHdCLiZDvAc/edit). ETS shall be responsible for determining the appropriateness of risk when the State Wide Area Network is involved. ETS shall determine the acceptability of risk when there is a perceived conflict between risks to the State Wide Area Network and the SLEDS Program’s assessment of risk. |

# 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 | 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 |  |
| Data Governance Committee |  |