



WYOMING
DEPARTMENT OF EDUCATION

*Creating Opportunities
for Students to Keep
Wyoming Strong*

Jillian Balow
Superintendent of Public Instruction

Dicky Shanor
Chief of Staff

Brent Bacon
Chief Academic Officer

Brent Young
Chief Policy Officer

Dianne Bailey
Chief Operations Officer



Cheyenne Office
Hathaway Building, 2nd Floor
2300 Capitol Avenue
Cheyenne WY 82002-0206
Phone: (307) 777-7690
Fax: (307) 777-6234

Riverton Office
320 West Main
Riverton, WY 82501
Phone: (307) 857-9250
Fax: (307) 857-9256

On the Web
edu.wyoming.gov
wyomingmeasuresup.com

Encryption Policy

Policy #: 4000-012

Version #: 2.0

Approved By: Jillian Balow, Superintendent, State of Wyoming
Department of Education

Effective Date: May 1, 2016

Purpose:

The purpose is to enforce a data in transit or at rest encryption mechanism for sensitive information whenever deemed appropriate.

Scope:

This policy applies to all WDE workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive student information. In addition, some third parties such as contractors or vendors may be required to abide by parts of or in whole this policy as indicated in contractual requirements.

Policy:

Portable WDE devices such as laptops will have full disk encryption in order to prevent any decipherable data retrieval in the event the device is lost, stolen, or otherwise access is attempted without proper authorization.

Encryption software will only be installed by an authorized member of the WDE technology team.

Encryption recovery keys will be stored in a secure location accessible by authorized WDE employees only

WDE employees will utilize authorized VPN access when establishing a connection to WDE resources from an external, to the wyo.gov, location

The WDE will balance the challenge of protecting “data at rest” against the increase in security technology complexity and administrative overhead including performance considerations and usability.

The WDE will review the viability of securing critical database, file servers as well as sensitive information on mobile devices such as laptops, phones and tablets.

The WDE will test encryption and decryption capabilities of products and systems to ensure proper functionality.

Responsibilities:

All workforce members are responsible for:

- Understanding and following all security related policies and procedures



WYOMING
DEPARTMENT OF EDUCATION



Jillian Balow

Superintendent of Public Instruction



Cheyenne Office

Hathaway Building, 2nd Floor
2300 Capitol Avenue
Cheyenne, WY 82002-0050
Phone: (307) 777-7675
Fax: (307) 777-6234

Casper Office

539 S. Payne
Casper, WY 82609
Phone: (307) 577-4686
Fax: (307) 577-6785

Riverton Office

320 West Main
Riverton, WY 82501
Phone: (307) 857-9253
Fax: (307) 857-9257

On the Web

edu.wyoming.gov
www.wyomingmeasuresup.com

The WDE Information Security Officer (ISO) is responsible for:

- Ensuring all workforce members understand and follow security related policies and procedures

Compliance:

It is the responsibility of the workforce member in custody of the portable device(s) to seek encryption implementation from a member of the WDE technology team. If the technology team fails to encrypt the device after a workforce member has requested such, and the member has not unreasonably inhibited the technology team from installing appropriate encryption software, workforce member will not be in violation of this policy.

Failure to comply with this or any other security policy will result in disciplinary actions as per HR Policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): None

Form(s): None

References:

- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- NIST 800-113, Guide to SSL VPNs;
<http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf>
- NIST 800-77, Guide to IPsec VPSs;
<http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf>
- NIST 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations;
<http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>
- NIST 800-111, Guide to Storage Encryption Technologies for End Users, <http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf>

Contact:

Aaron Roberts

E: aaron.roberts@wyo.gov
P: 307-777-8014
F: 307-777-6234

Policy History: Initial effective date: May 1, 2016