



Department of Education/Vermont Data Consortium

Education Data Warehouse & Analyzer

Policies and Procedures

TABLE OF CONTENTS

I. INTRODUCTION	2
II. AUDIENCE	3
III. PURPOSE	3
IV. DEFINITIONS	4
V. ACCEPTABLE USAGE OF THE WAREHOUSE	6
VI. SECURITY OF THE WAREHOUSE	9
VII. MAINTENANCE AND SUPPORT OF THE WAREHOUSE	12
VIII. APPENDIX A: FERPA SUMMARY	14
IX. APPENDIX B: EDWA POLICY AND PROCEDURE ACCEPTANCE.....	17
X. APPENDIX C: USER ACCESS REQUEST FORM.....	18
XI. APPENDIX D: DATA REQUEST FORM.....	20

I. INTRODUCTION

Vermont educators have always had questions about the factors that influence student achievement. How does preschool participation affect student performance in later grades? What are the effects of intervention programs? What is the cost benefit of the new math program? What is the relationship of class size to student performance? The Vermont Department of Education collects information from schools in order to meet state and federal reporting requirements but this information can also be leveraged to answer questions like, “What is the effect of professional development on writing scores?” “What are the areas that schools need support in?” Vermont families want to know, “How are the 4th graders performing at my child’s school?” “How does my child’s school perform in comparison to other Vermont schools?”

As partners in the Vermont education system we all want our students to become productive members of the 21st century, meeting or exceeding state and national standards. The Vermont Department of Education and the Vermont Data Consortium are developing a state of the art Education Data Warehouse & Analyzer to assist us in making decisions that will help us accomplish this task. For the first time, we will be able to efficiently analyze the relationship between our educational efforts, demographics, professional development, perception data, and student performance, to inform decisions that we make about curriculum, budget, programs, professional development, etc. The Education Data Warehouse and analyzer tools are being made available to Vermont educators, the Vermont Department of Education in an effort to improve student achievement and well-being and deliver the best education to our students in a cost efficient, equitable manner. The Education Data Warehouse will provide this capability via a safe and secure manner, protecting the privacy of our students. Different types of users will have varying levels of access to the Education Data Warehouse. In addition, a public portal will allow citizens to access public information about our schools and districts.

As part of our ongoing effort to responsibly use educational data as part of the school improvement process, it is of the utmost importance for all Education Data Warehouse users to be aware that rigorous policies and procedures need to be in place before anyone, at any level, accesses our student data. This document defines secure and acceptable use of the Educational Data Warehouse and outlines standards, procedures and best practices for using it safely. It contains examples of what to do and what not to do to safeguard student data and use it appropriately for educational analysis. This document also outlines how to report a problem, manage your data and how to get help. The education data warehouse will not provide access to confidential student data beyond what is currently permitted via users’ current job roles. The education data warehouse allows for precise control of data access and also has the ability to track how users are utilizing this powerful tool. It is the responsibility of each and every user to read and understand the contents of this document and with your signature, agree to access the warehouse in accordance with its rules in order to keep our children and their information safe.

II. AUDIENCE

The intended audience of this document includes all users and administrators of the Education Data Warehouse & Analyzer tool (EDWA) and TetraData's EASE-e web-browser application, which is the access point or portal into the EDWA.

Staff from the following are expected to comprise the user group:

1. State of Vermont, Department of Education (DOE)
2. Vermont Data Consortium (VDC)
3. Educators
4. Education Administrators
5. Public Users

This document applies to #1 through #4 above. The data available through the Public User Portal does not fall under the guidelines of this Policies and Procedures document.

We further anticipate that each user will be placed into one of the following groups, in order for security and access to be managed effectively:

1. General User: Has access to view basic data within EDWA.
2. Power User: Has access to view basic and advanced data within EDWA.
3. Data Administrator: Has access to all data within EDWA, and can ADD, CHANGE, and REMOVE data within the EDWA. Manages and completes user requests for data manipulation (ADD, CHANGE, REMOVE).
4. System Administrator: Establishes user accounts, user rights, and audits EDWA usage.
5. EDWA Sponsors: DOE and VDC are the sponsors of the EDWA.

III. PURPOSE

The purpose of establishing a Policies and Procedures manual is to ensure:

1. Information in the EDWA is protected from improper access and use following the guidelines set forth in the Family Educational Rights and Privacy Act (FERPA);
2. Prevention of the inappropriate and unauthorized disclosure of information and avoidance of adverse legal consequences;
3. The user community is informed about confidentiality, privacy, and acceptable use of the EDWA.

IV. DEFINITIONS

This section defines terms used throughout this document and/or terms you may see through your usage of the EDWA.

Is it a Policy, a Standard or a Guideline?

What's in a name? We may hear people use the names "policy", "standard", and "guideline" to refer to documents that fall within the policy infrastructure. So that those who participate in this process can communicate effectively, we'll use the following definitions.

A policy is typically a document that outlines specific requirements or rules that must be met. In the data usage realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the data set within the data warehouse.

A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone. For example, you might have a standard that describes how to request a new data set be added to the data warehouse. People must follow this standard exactly if they wish to add a data set to the data warehouse.

A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met, but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

Access Control

Access Control ensures that resources are only granted to those users who are entitled to them.

Data Encryption Standard (DES)

A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Data Warehousing

Data Warehousing is the consolidation of several previously independent databases into one location.

Denial of Service (DOS)

The prevention of authorized access to a system resource or the delaying of system operations and functions.

FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Gateway

A network point that acts as an entrance to another network.

Internet Protocol (IP)

The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec)

A developing standard for security at the network or packet processing layer of network communication.

Risk

Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Assessment

A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

Safety

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

Secure Sockets Layer (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Sensitive Information

Sensitive information is any information that, if compromised or disclosed, could adversely affect the DOE/VDC's interest or credibility, could be used to discriminate unfairly against any person, or groups within the community, or could be used to identify an individual protected by FERPA.

V. ACCEPTABLE USAGE OF THE WAREHOUSE

This section describes what is deemed acceptable use of the data within the EDWA as well as acceptable use of TetraData's EASE-e™ Analysis Suite, which is the point of access or portal into the EDWA.

In some instances we provide examples of unacceptable and acceptable usage. These are only examples to provide some context and do NOT comprise a complete list.

ACCEPTABLE USE

All personally identifiable information contained in all student education records, including information available through the EDWA, is confidential and prohibited from disclosure except as permitted by the Federal Family Educational Rights and Privacy Act (FERPA). Information/data and systems may only be used by authorized individuals to accomplish tasks related to their jobs. Use of the information and systems for personal gain, personal business, or to commit fraud is prohibited.

Information not classified as **PUBLIC** must be protected, and must not be disclosed without authorization. Unauthorized access, manipulation, disclosure, or secondary release of such information constitutes a security breach, and may be grounds for disciplinary action up to and including termination of employment in accordance with your SU or DOE policies.

Pending your acceptance of this document and approval of your request to obtain an EDWA user account (see Appendix B), you will be given access to information contained in the EDWA solely for the purpose of fulfilling official job duties. You agree to keep all information in a manner that is appropriate to its content and to keep any personally identifiable information confidential, kept out of public view, and stored in a secure location/form, whether it is in paper copy, contained in software, visible on screen displays, in computer readable, or any other form. You understand you are solely responsible for the use of this information, including its disclosure to others. You therefore agree not to re-disclose or provide access to this information except as authorized by your job duties and in compliance with federal and state laws and this policy. Neither curiosity nor personal relationships provide a basis for any breach of confidentiality.

By signing this document and receiving confirmation of your user account activation, you acknowledge you are the only authorized user of the assigned EDWA account, and that you will take steps to maintain the security, confidentiality, and integrity of any information accessed by you. These steps include protecting the confidentiality of your password to ensure others may not use it to access your account. You understand that you are responsible for receiving training on all data subsets to which you have been given access in the EDWA . If you do not comply with the training requirement, your account may be revoked. You understand that, because the data is transferred periodically from a transactional computer system to the EDWA, the information you receive may not be current.

Examples of Acceptable Use include:

1. While using someone else's computer, you connect to the EDWA. When you have finished, you log off of your account, closing any browser windows you may have used, and making sure your password was not saved on the computer;
2. Use of the EDWA for data analysis as it relates to your job.

Examples of Unacceptable Use include:

1. Leaving EDWA screen open on an unattended desktop;
2. Sharing information with other people who are not authorized to see it;
3. Accessing information that you are not authorized to view;
4. Accessing information that you have authorization to BUT for inappropriate reasons, e.g. looking up a neighbor's children's test results;
5. While someone else is using a computer, you want to check something in the EDWA. You ask them to log in, giving them your password to type in for you;
6. Emailing reports or saving a shared query with student identifying information;
7. Lack of diligence in securing user names or passwords (i.e. leaving password written under keyboard, or using a password that is easy to guess. e.g. your child's or pet's name.

THE ABOVE ACCEPTABLE AND UNACCEPTABLE USE EXAMPLES ARE JUST THAT, EXAMPLES, AND DO NOT COMPRISE A COMPLETE LIST.

Please note that school districts are not subject to the Freedom of Information Act. VT public record law says that they need only provide access to existing non-confidential reports. FERPA protects reports if they contain confidential information. School district staff should escalate requests to their Superintendent Office who will confer with attorneys as needed.

MONITORING OF USE

DOE/VDC reserves the right to monitor access to the EDWA by authorized user(s), as part of the normal course of its business practice. Should DOE/VDC discover User(s) engaged in prohibited actions, which create denial of access or impediment of service, and which adversely affect DOE/VDC's ability to provide services, DOE/VDC reserves the right to temporarily suspend User/Licensee access to the EDWA. DOE/VDC shall make written/electronic notification to User point of contact of any temporary suspension, and the cause thereof, as soon as reasonably possible.

WARRANTY

You expressly understand and agree that the EDWA is provided on an "AS IS" and "AS AVAILABLE" basis. DOE/VDC makes no representations or warranties of any kind, expressed or implied as to the operation of this site or the information, content, materials, or products included on this site. You expressly agree that your use of this site is at your sole risk to the full extent permissible by applicable law, DOE/VDC disclaims all warranties, expressed or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose and non-infringement. DOE/VDC does not warrant that this site and data are free of viruses or other harmful components. DOE/VDC will not be liable for any damages of any kind arising from the use of this site, including but not limited to direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for lost profits, goodwill, use, data or other intangibles resulting from:

- I) the use or inability to use the site;
- II) the cost of procurement of substitute goods and services resulting from any goods, data, information or services purchased or obtained or messages received or transactions entered into through or from the site;
- III) unauthorized access to or alteration of your transmissions or data;
- IV) statements or conduct of any third party on the service; or
- V) any other matter relating to the service.

VI. SECURITY OF THE WAREHOUSE

AUDIENCE: Data Users and Data Keepers

The Minimum Standards described are the minimum recommended action steps, while the Best Practices assume the Minimum Standards are met, and adds additional action steps.

PASSWORD PROTECTION:

The following highlights the Minimum Standards and Guidelines / Best Practices to follow regarding password usage.

Minimum Standards:

Minimum password standards dictate that passwords:

1. ARE used (do not leave your password blank)
2. ARE changed at least every 90 days
3. ARE NOT the word "password"
4. ARE NOT the same name as your user account
5. ARE NOT used more than one time within the past 5 password changes
6. ARE NOT changed more than once per day

When possible, the EDWA application will enforce these standards. All other applications used to secure desktop and access data should address these password standards where possible.

Guidelines / Best Practices:

Common passwords, based on letters and numbers can typically be recovered in about a day using the default character set A-Z and 0-9. Complex passwords, on the other hand, that use characters such as #_}* may take up to hundreds of days to crack on the same machine, using a comprehensive character set. See the link for examples of password cracking: <http://www.mcmaster.ca/cis/ITsecurity/passwordcracking.htm>

It is important to realize that short passwords, and easily guessed longer passwords, are virtually useless. If you haven't changed your approach to passwords in the last few years, this might be a good time to do just that -- and to look at the tools that make generating and using even very long, highly-secure passwords much easier.

If you'd rather keep your password-generation local and offline, use the open source "PWGen for Windows" at <http://pwgen-win.sourceforge.net> or RoboForm at <http://www.roboform.com>.

In summary, it is Best Practice to use a password that:

1. IS NOT a word found in the dictionary
2. IS a combination of letters and numbers
3. IS a combination of upper and lower case letters
4. IS a minimum of 6 characters
5. IS never saved when prompted to 'Remember Password'.

COMPUTER PROTECTION:

The following highlights the Minimum Standards and Best Practices to proactively protect your computer from a security breach, which would otherwise lead to a potential breach of the EDWA.

Minimum Standards:

1. Ensure that current anti-virus and current signature files (daily definition updates) are installed
2. Don't open e-mail or attachments from people you don't know or are not expecting e-mail from – especially if the e-mail contains an attachment. If you are not sure of the sender delete the message
3. Enable real-time e-mail scanning by your virus checker
4. Do NOT unsubscribe to spam e-mail. While this seems like a way to stop a spammer from sending more mail to you, it only serves to validate that the spammer has a legitimate e-mail address for you
5. If supported, configure browser to not save username/password cookies
6. Use the screen saver capability of desktop to automatically lock desktop after 5 minutes of inactivity.

Guidelines / Best Practices:

1. Install a personal firewall on your PC (PC is used to identify a personal computer, be it an IBM-compatible PC or an Apple PC);
2. When directed by your IT staff, update the Operating System (i.e. Windows, OS X) with most current patches;
3. Do NOT setup your email Inbox for AutoPreview or Preview Pane. This could cause your system to become infected if there is a virus in the message body;
4. Run Anti-Spyware software;

DOE IT will ensure all DOE issued laptops and computers will be configured to be protected by the Minimum Standards #1 and #3 and Guidelines / Best Practices #1 and #2. DOE will continue to review current technology and automatically implement whatever protections are possible on DOE issued laptops. Appropriate behavior is required to ensure these protections stay activated.

VDC users should contact their IT support team to find out what protections are in place on systems provided to them. Appropriate behavior is required to ensure these protections stay activated.

We strongly encourage you to implement similar protections on your home computers.

CONFIDENTIALITY AGREEMENTS:

FERPA establishes the guidelines for data confidentiality of the EDWA. See Appendix A for additional information.

VII. MAINTENANCE AND SUPPORT OF THE WAREHOUSE

AUDIENCE: Data Users and Data Keepers

HOW TO...:

1. How To Report A Security Breach

- a. If you become aware of a security breach, be it unauthorized usage of data, unauthorized access to the EDWA, or some other suspicious activity related to the EDWA, please email edwa@education.state.vt.us.

2. How To Get Help

- a. The VDC and DOE will provide first line support to their respective user base. Unresolved issues will be passed onto TetraData for resolution. The appropriate first line support personnel will track all issues until resolved.
- b. For DOE users, specific individuals will be designated as their area's coaches to provide first line support on all 'How to' and data questions. These coaches will be posted on <http://doeweb/>. Other support instructions are available on DOEWEB as well.
- c. VDC Users: Please see www.vermontdata.org for the steps to follow to get support.

3. How To Get a User Account on the EDWA (Access Request)

- a. See Appendix C. Check <http://doeweb/> or www.vermontdata.org for latest form.

4. How To Get Access to Data Sets on the EDWA (Access Change/Control)

- a. See Appendix C. Check <http://doeweb/> or www.vermontdata.org for latest form.

5. How To Add, Change, Remove Data and Reports within the EDWA

- a. See Appendix D. Check <http://doeweb/> or www.vermontdata.org for latest form.

6. Information Owner Policy

DOE/VDC will ensure that there is a registered Information Owner (IO) that will:

1. be assigned for each information source, e.g. application, database, data table, data element, report, etc.
2. be responsible for insuring the validity of their information
3. be responsible for ensuring all new systems affecting their information meet their requirements
4. be responsible for approving all Access Request and Change Access to their information

5. be responsible for periodic Access Review of all who have access to their information to ensure access is still appropriate
6. be responsible for reviewing / approving all New Data Load and Report Request and Change Request that impact their information
7. be responsible for determining criticality of their information and business continuity planning if information is mission critical.

7. Access Review Policy

DOE/VDC will periodically initiate a review, or audit, of data usage of the EDWA, to understand levels of usage and ensure data access is consistent with defined Access Control definitions. The Information Owner(s) will review, make changes, and sign off on this access and use.

8. Risk Assessment Policy

DOE/VDC will periodically initiate a review, or audit, of the security model of the EDWA, to identify, assess, and remediate risks to the organization's information infrastructure associated with conducting business.

9. Audit Vulnerability Scanning Policy

DOE/VDC will periodically initiate a review, or audit, of risk assessment to ensure integrity of information/resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.

VIII. APPENDIX A: FERPA SUMMARY

This section provides a summary of FERPA: Family Educational Rights and Privacy Act.

Please see: <http://www.ed.gov/policy/gen/reg/ferpa/index.html> for more information.

SUMMARY

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31¹):

1. School officials with legitimate educational interest;
2. Other schools to which a student is transferring;
3. Specified officials for audit or evaluation purposes;
4. Appropriate parties in connection with financial aid to a student;
5. Organizations conducting certain studies for or on behalf of the school;
6. Accrediting organizations;
7. To comply with a judicial order or lawfully issued subpoena;
8. Appropriate officials in cases of health and safety emergencies; and
9. State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of

¹ Please review the regulations at <http://www.ed.gov/policy/gen/reg/ferpa/index.html> for the specific conditions.

notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

FERPA INDEX

Title 34--EDUCATION

Subpart A_General

- 99.1 To which educational agencies or institutions do these regulations apply?
- 99.2 What is the purpose of these regulations?
- 99.3 What definitions apply to these regulations?
- 99.4 What are the rights of parents?
- 99.5 What are the rights of students?
- 99.6 [Reserved]
- 99.7 What must an educational agency or institution include in its annual notification?
- 99.8 What provisions apply to records of a law enforcement unit?

Subpart B_What Are the Rights of Inspection and Review of Education Records?

- 99.10 What rights exist for a parent or eligible student to inspect and review education records?
- 99.11 May an educational agency or institution charge a fee for copies of education records?
- 99.12 What limitations exist on the right to inspect and review records?

Subpart C_What Are the Procedures for Amending Education Records?

- 99.20 How can a parent or eligible student request amendment of the student's education records?
- 99.21 Under what conditions does a parent or eligible student have the right to a hearing?
- 99.22 What minimum requirements exist for the conduct of a hearing?

Subpart D_May an Educational Agency or Institution Disclose Personally Identifiable Information From Education Records?

- 99.30 Under what conditions is prior consent required to disclose information?
- 99.31 Under what conditions is prior consent not required to disclose information?
- 99.32 What recordkeeping requirements exist concerning requests and disclosures?
- 99.33 What limitations apply to the redisclosure of information?
- 99.34 What conditions apply to disclosure of information to other educational agencies or institutions?
- 99.35 What conditions apply to disclosure of information for Federal or State program purposes?

- 99.36 What conditions apply to disclosure of information in health and safety emergencies?
- 99.37 What conditions apply to disclosing directory information?
- 99.38 What conditions apply to disclosure of information as permitted by State statute adopted after November 19, 1974, concerning the juvenile justice system?
- 99.39 What definitions apply to the nonconsensual disclosure of records by postsecondary educational institutions in connection with disciplinary proceedings concerning crimes of violence or non-forcible sex offenses?

Subpart E_What Are the Enforcement Procedures?

- 99.60 What functions has the Secretary delegated to the Office and to the Office of Administrative Law Judges?
- 99.61 What responsibility does an educational agency or institution have concerning conflict with State or local laws?
- 99.62 What information must an educational agency or institution submit to the Office?
- 99.63 Where are complaints filed?
- 99.64 What is the complaint procedure?
- 99.65 What is the content of the notice of complaint issued by the Office?
- 99.66 What are the responsibilities of the Office in the enforcement process?
- 99.67 How does the Secretary enforce decisions?

Appendix A to Part 99--Crimes of Violence Definitions

Authority: 20 U.S.C. 1232g, unless otherwise noted.

Source: 53 FR 11943, Apr. 11, 1988, unless otherwise noted.

IX. APPENDIX B: EDWA POLICY AND PROCEDURE ACCEPTANCE

I have read the Education Data Warehouse & Analyzer Policies and Procedures document, I have had the opportunity to have my questions regarding these policies, and my access to and use of the Information answered.

I understand that providing information for unauthorized uses or otherwise violating confidentiality policies relating to the information may limit my access to the EDWA, and/or result in disciplinary action, including my dismissal and prosecution under applicable federal or state laws.

Applicant: _____ Date: _____
Print Name

Applicant: _____ Date: _____
Signature

EDWA Administrator
(or Designee): _____ Date: _____
Print name

EDWA Administrator
(or Designee): _____ Date: _____
Signature

DOE users should sign and turn this form into IT.
VDC users should sign and turn this form into their VDC representative or VDC trainer.

X. APPENDIX C: USER ACCESS REQUEST FORM

The following form is an example of the form to be used to submit your request to gain or change access to the EDWA. Please use the latest form available on the internal DOEWEB site and VDC site at www.vermontdata.org.

EDWA User Access Request Form

PART A: User Information (to be completed by Requester and approved by Manager)			
Type of Request:	New User: <input type="checkbox"/>	Access Change: <input type="checkbox"/>	Remove Access: <input type="checkbox"/>
Request Date:	<input type="text"/>	Required Date *:	<input type="text"/>
Name:	<input type="text"/>	Priority:	HIGH
Job Title:	<input type="text"/>	User Name for Login:	<input type="text"/>
Phone Number:	<input type="text"/>	Email:	<input type="text"/>
Domain:	DOE	Physical Location:	<input type="text"/>
Role/Area (Enter as many Area/Role combinations as are applicable, using the information described on the next page. Enter in the format: <i>Role/Area</i> <input type="text"/> Or...assign access just like this person's <input type="text"/>	If Domain is VDC, specify ORG list:		<input type="text"/>
Teacher ID (if role is TEACHER):	<input type="text"/>		
Manager Name:	<input type="text"/>	Manager Sign Off: (Indicates Manager Approval)	<input type="checkbox"/>
Describe Access Required (fill out this section with specifics if a new Role/Area combination is needed):			
PART B : Approval (to be completed by DOE/VDC)			
Information Owner (IO) Name:	<input type="text"/>	IO Sign Off: (Indicates IO approval)	<input type="checkbox"/>
DOE/VDC Sign Off By:	<input type="text"/>	Date:	<input type="text"/>
Comments:	<input type="text"/>		
PART C : Implementation (to be completed by DOE/VDC)			
Implemented By:	<input type="text"/>	Date:	<input type="text"/>
Comments:	<input type="text"/>		

DOE requesters should refer to <http://doeweb/> for help and where to send form.

VDC requesters should refer to www.vermontdata.org for help and where to send form.

What the Domain / Role / Area Assignments Mean for EDWA Data Access

DOMAIN – select only one per user setup.

- **DOE** – has security access* to all organizations
- **VDC** – has security access* to specified organizations

Security access – will have student level access based on ROLE and AREA logic below, else will only see data at the organization level with small-n sample size suppression activated unless otherwise noted below.

The below **ROLE/AREA** assignments must be specified together. For example, Admin/Assessment, User/Tech Ed. More than one role/area assignment per user is allowed.

ROLE

- **Admin** – has access to student level AND student identifying information (names, id). Unless overridden by AREA security below, small-n sample size suppression is not activated, i.e. will see a number < 10 in a report cell.
- **Analyst** – has access to student level BUT NOT student identifying information (no names/id). Unless overridden by AREA security below, small-n sample size suppression is not activated, i.e. will see a number < 10 in a report cell.
- **User** – For DOE domain Users, does not have access to student level or student identifying information, all access is at organization level. Unless overridden by AREA security below, small-n sample size suppression is activated, i.e. will NOT see a number < 10 in a report cell. VDC domain Users will have student level access to only their organizations' students with organization level and small-n suppression for other organizations.
- **Teacher** – For VDC domain use only. Student level and identifying information restricted to current students. Former students can be viewed only if in same administrative organization.

AREA

- **Public** – all data is accessed at organization level only with small-n sample size suppression activated, i.e. will NOT see a number < 10 in a report cell. Only sees Yes/No flags for SPED, ELL, and Migrant.
- **Org** – can see all organization, student and educator information. Identifying information is available AND small-n suppression is not activated.
- **SPED** – can see student information for SPED students only.
- **ELL** – can see student information for ELL students only. No access to Discipline and Educator objects.
- **Migrant** – can see student information for Migrant students only. No access to Discipline and Educator objects.
- **Tech Ed** – can see student information for Tech Ed students only. No access to Discipline objects.
- **Assessment** – has access to student level data. Only sees Yes/No flags for SPED, ELL, and Migrant. **Admin** can see SPED – Disability attributes. **User** does not have small-n suppression activated. Does not have access to Educator, Discipline and Tech Ed data.
- **DMAT** – has access to Organization, Student and Educator objects, except for AYP, SPED and Tec Ed. Only **Admin** has access to tests.
- **Finance** – has organization level access only to Student objects. No access to tests, educator or discipline objects. Place holder for future access to Financial data sets.
- **SHS** – has full access to YRBS and Discipline objects. Organization level access only to all other student and educator objects.
- **AHS** – has full access to YRBS and Discipline objects. Small-n sample size suppression always activated for student object and test objects regardless of ROLE.
- **EQ** – has full access to Educator objects.
- **HR** – for future VDC domain use.
- **Curr** – for future VDC domain use

XI. APPENDIX D: DATA REQUEST FORM

The following form is an example of the form to be used to submit your request to add/change/remove data and reports within the EDWA. Please use the latest form available on the internal DOEWEB site and VDC site at www.vermontdata.org.

EDWA Data and Report Request Form

PART A: Data Request Information (to be completed by Requester and approved by Manager)				
Type of Request:	Data Add: <input type="checkbox"/>		Data Change: <input type="checkbox"/>	Remove Data: <input type="checkbox"/>
	Report Add: <input type="checkbox"/>		Report Change: <input type="checkbox"/>	Remove Report: <input type="checkbox"/>
Request Date:	<input type="text"/>	Required Date *:	<input type="text"/>	Priority: HIGH
Name:	<input type="text"/>		Job Title:	<input type="text"/>
Email:	<input type="text"/>		Phone Number:	<input type="text"/>
Manager Name:	<input type="text"/>		Manager Sign Off: (Indicates Manager Approval)	<input type="checkbox"/>
Describe Details of Request: ¹ <input type="text"/>				
Describe Benefits of Request: ² <input type="text"/>				
PART B : Review and Approval (to be completed by DOE/VDC)				
Information Owner (IO) Name:	<input type="text"/>			IO Sign Off: (Indicates IO approval) <input type="checkbox"/>
DOE/VDC Sign Off By:	<input type="text"/>	Date:	<input type="text"/>	
Comments (describe the planned implementation approach and estimated schedule) :	<input type="text"/>			
PART C : Implementation (to be completed by DOE/VDC)				
Implemented By:	<input type="text"/>	Date:	<input type="text"/>	
Comments:	<input type="text"/>			

DOE requesters should refer to <http://doeweb/> for help and where to send form.

VDC requesters should refer to www.vermontdata.org for help and where to send form.

¹ Provide requirement details on data sources, frequency, user base, security, etc. Please provide enough information to allow for request review, approval and prioritization.

² Provide details on the benefits expected from request implementation, e.g. any cost savings, accuracy and efficiencies gained, etc. Please provide enough information to allow for request review, approval and prioritization.