



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER
EHS10018

PAGE
1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
ROBERTA WAGNER 304-558-0067

VENDOR

RFQ COPY
 TYPE NAME/ADDRESS HERE

SHIP TO

HEALTH AND HUMAN RESOURCES
 BPH ENVIRO HLTH SERVICES
 CAPITOL AND WASHINGTON STREETS
 1 DAVIS SQUARE, SUITE 200
 CHARLESTON, WV
 25301-1798 304-558-2981

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
09/21/2009				

BID OPENING DATE: 10/07/2009 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
ADDENDUM NO. 1						
1. QUESTIONS AND ANSWERS ARE ATTACHED.						
2. TO MOVE BID OPENING DATE FROM 9/24/2009 TO 10/7/2009.						
3. ADDENDUM ACKNOWLEDGEMENT IS ATTACHED. THIS DOCUMENT SHOULD BE SIGNED AND RETURNED WITH YOUR BID. FAILURE TO SIGN AND RETURN MAY RESULT IN DISQUALIFICATION OF YOUR BID.						
EXHIBIT 10						
REQUISITION NO.: EHS10018						
ADDENDUM ACKNOWLEDGEMENT						
I HEREBY ACKNOWLEDGE RECEIPT OF THE FOLLOWING CHECKED ADDENDUM(S) AND HAVE MADE THE NECESSARY REVISIONS TO MY PROPOSAL, PLANS AND/OR SPECIFICATION, ETC.						
ADDENDUM NO. S:						
NO. 1						
NO. 2						
NO. 3						
NO. 4						
NO. 5						
I UNDERSTAND THAT FAILURE TO CONFIRM THE RECEIPT OF THE ADDENDUM(S) MAY BE CAUSE FOR REJECTION OF BIDS.						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
-----------	-----------	------

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE
-------	------	-----------------------------------

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

**GENERAL TERMS & CONDITIONS
REQUEST FOR QUOTATION (RFQ) AND REQUEST FOR PROPOSAL (RFP)**

1. Awards will be made in the best interest of the State of West Virginia.
2. The State may accept or reject in part, or in whole, any bid.
3. All quotations are governed by the *West Virginia Code* and the *Legislative Rules* of the Purchasing Division.
4. Prior to any award, the apparent successful vendor must be properly registered with the Purchasing Division and have paid the required \$125 fee.
5. All services performed or goods delivered under State Purchase Order/Contracts are to be continued for the term of the Purchase Order/Contracts, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise available for these services or goods, this Purchase Order/Contract becomes void and of no effect after June 30.
6. Payment may only be made after the delivery and acceptance of goods or services.
7. Interest may be paid for late payment in accordance with the *West Virginia Code*.
8. Vendor preference will be granted upon written request in accordance with the *West Virginia Code*.
9. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.
10. The Director of Purchasing may cancel any Purchase Order/Contract upon 30 days written notice to the seller.
11. The laws of the State of West Virginia and the *Legislative Rules* of the Purchasing Division shall govern all rights and duties under the Contract, including without limitation the validity of this Purchase Order/Contract.
12. Any reference to automatic renewal is hereby deleted. The Contract may be renewed only upon mutual written agreement of the parties.
13. **BANKRUPTCY:** In the event the vendor/contractor files for bankruptcy protection, the State may deem this contract null and void, and terminate such contract without further order.
14. **HIPAA BUSINESS ASSOCIATE ADDENDUM:** The West Virginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, and available online at the Purchasing Division's web site (<http://www.state.wv.us/admin/purchase/vrc/hipaa.htm>) is hereby made part of the agreement. Provided that, the Agency meets the definition of a Cover Entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the vendor.
15. **WEST VIRGINIA ALCOHOL & DRUG-FREE WORKPLACE ACT:** If this Contract constitutes a public improvement construction contract as set forth in Article 1D, Chapter 21 of the West Virginia Code ("The West Virginia Alcohol and Drug-Free Workplace Act"), then the following language shall hereby become part of this Contract: "The contractor and its subcontractors shall implement and maintain a written drug-free workplace policy in compliance with the West Virginia Alcohol and Drug-Free Workplace Act, as set forth in Article 1D, Chapter 21 of the West Virginia Code. The contractor and its subcontractors shall provide a sworn statement in writing, under the penalties of perjury, that they maintain a valid drug-free workplace policy in compliance with the West Virginia Alcohol and Drug-Free Workplace Act. It is understood and agreed that this Contract shall be cancelled by the awarding authority if the Contractor: 1) Fails to implement its drug-free workplace policy; 2) Fails to provide information regarding implementation of the contractor's drug-free workplace policy at the request of the public authority; or 3) Provides to the public authority false information regarding the contractor's drug-free workplace policy."

INSTRUCTIONS TO BIDDERS

1. Use the quotation forms provided by the Purchasing Division.
2. **SPECIFICATIONS:** Items offered must be in compliance with the specifications. Any deviation from the specifications must be clearly indicated by the bidder. Alternates offered by the bidder as **EQUAL** to the specifications must be clearly defined. A bidder offering an alternate should attach complete specifications and literature to the bid. The Purchasing Division may waive minor deviations to specifications.
3. Complete all sections of the quotation form.
4. Unit prices shall prevail in case of discrepancy.
5. All quotations are considered F.O.B. destination unless alternate shipping terms are clearly identified in the quotation.
6. **BID SUBMISSION:** All quotations must be delivered by the bidder to the office listed below prior to the date and time of the bid opening. Failure of the bidder to deliver the quotations on time will result in bid disqualifications: Department of Administration, Purchasing Division, 2019 Washington Street East, P.O. Box 50130, Charleston, WV 25305-0130



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER
EHS10018

PAGE
2

ADDRESS CORRESPONDENCE TO ATTENTION OF:
ROBERTA WAGNER 304-558-0067

RFQ COPY
 TYPE NAME/ADDRESS HERE

VENDOR

SHIP TO

HEALTH AND HUMAN RESOURCES
 BPH ENVIRO HLTH SERVICES
 CAPITOL AND WASHINGTON STREETS
 1 DAVIS SQUARE, SUITE 200
 CHARLESTON, WV
 25301-1798 304-558-2981

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
09/21/2009				

BID OPENING DATE: 10/07/2009 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>VENDOR MUST CLEARLY UNDERSTAND THAT ANY VERBAL REPRESENTATION MADE OR ASSUMED TO BE MADE DURING ANY ORAL DISCUSSION HELD BETWEEN VENDOR'S REPRESENTATIVES AND ANY STATE PERSONNEL IS NOT BINDING. ONLY THE INFORMATION ISSUED IN WRITING AND ADDED TO THE SPECIFICATIONS BY AN OFFICIAL ADDENDUM IS BINDING.</p> <p>..... SIGNATURE COMPANY DATE</p> <p>REV. 11/96</p> <p>END OF ADDENDUM NO. 1</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER
EHS10018

PAGE
3

ADDRESS CORRESPONDENCE TO ATTENTION OF:
ROBERTA WAGNER 304-558-0067

RFQ COPY
 TYPE NAME/ADDRESS HERE

VENDOR

SHIP TO

HEALTH AND HUMAN RESOURCES
 BPH ENVIRO HLTH SERVICES
 CAPITOL AND WASHINGTON STREETS
 1 DAVIS SQUARE, SUITE 200
 CHARLESTON, WV
 25301-1798 304-558-2981

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
09/21/2009				

BID OPENING DATE: 10/07/2009 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	1	LB		220-34		
TO DEVELOP & IMPLEMENT A CENTRALIZE DATA MODE EXCHAN						
***** THIS IS THE END OF RFQ EHS10018 ***** TOTAL:						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
-----------	-----------	------

TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE
-------	------	-----------------------------------

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

EHS10018 Addendum #1 - TO ANSWER VENDOR QUESTIONS RELATED TO THE ORIGINAL REQUEST FOR QUOTATION.

1. Section III mentions "In the event that the total cost of the completed project exceeds the funds available, deliverable [4] may be deducted." Can you provide the maximum funds available for this project?

Response: WV policy prohibits release of the maximum funds available.

2. Deliverable #2 mentions implementation of "Lab to State" software. Is this strictly limited to the implementation of EPA's "Lab to State" software (http://www.epa.gov/ogwdw000/sdwis_st/current.html) or will WVDHHR allow implementation of other 3rd party Lab-to-State e-reporting solutions that also integrate with SDWIS/State?

Response: This contract is strictly limited to the specified Lab to State software.

3. Can you provide a copy of your existing Laboratory and MOR forms?

Response: There is not a standard laboratory form. The MOR forms are available at <http://www.wvdhhr.org/oehs/eed/c&e/mor.asp>

4. Section IV mentions WV Office of Technology and WV DHHR security policies for IT services. Can you provide a copy of these policies?

Response: The WV Office of Technology policies can be found at: <http://www.state.wv.us/ot/article2.cfm?atl=82E13BB8-9E19-5AF4-2845EB154B1C0142&fs=1>

The WV DHHR polices listed below are be attached.

0511 - IT Network Security - revised 01/05/04

0512 - IT Information Security - effective 4/15/03

Attachment A - Roles and Responsibilities

IT-0513 - Physical Security for IT Resources - effective 4/18/05

IT-0519 - Data Transmission Security and Integrity - effective 4/15/05

OP-14 - User Security - revised 5/18/05

OP-21 - Security Management Process - effective 4/12/05

OP-22 - Information Security Awareness Training - effective 4/15/05

5. Deliverable #4 calls for the implementation of SWOCS software. Is this limited to a particular SWOCS software, or will WVDHHR allow implementation of other 3rd party SWOCS solutions? Does WV DHHR already have the SWOCS software purchased and looking for implementation only, or does this deliverable cover both the software + implementation?

Response: SWOCS software is installed and operational. This contract is to allow specified users to "view" existing information that is within the software tables.

6. The method of award indicates that it is solely based on lowest price among qualified responses. Can WV DHHR provide the criteria/scoring for determining that a responder is qualified?

Response: This award will be awarded based upon the lowest bidder that meets all required specifications and requirements as written in the RFQ. There is no criteria/scoring that will be used to determine the qualified respondent.

7. Is this ongoing work or continuation of work conducted by a previous contractor?

Response: This proposal is for new work and this is not continuation of work conducted by a previous contractor.

8. Where can the WV security and IT service and application policies be found?

Response: The WV Office of Technology policies can be found at:
<http://www.state.wv.us/ot/article2.cfm?atl=82E13BB8-9E19-5AF4-2845EB154B1C0142&fs=1>

9. What is the current node developed in Java, .NET, etc?

Response: There is no current node. There is a server available to install the node.

10. Who is the manufacturer of the current 1.1 node?

Response: There is no current 1.1 Node.

11. What technologies and databases are supported by the WV DHHR IT environment (e.g. Java, .NET, Oracle, SQL Server)?

Response: The technology and databases currently supported by WV DHHR IT are JAVA and Oracle 10g DB, Oracle Application Server 10g.

12. Does the Node 2.0 need to be implemented using a specific technology and/or database?

Response: Node 2.0 needs to be implemented using JAVA and Oracle 10g DB, and Oracle Application Server 10g.

13. Is WV using the current EPA Lab to State software available through EPA SDWIS? If not, is the database of Lab to State for Laboratories accessible and what is the type of database used? What is the technology(s) behind the Lab to State for Laboratories software?

Response:

1. No we are not currently using the EPA lab to state software because we are not accepting electronic laboratory results but when we do accept electronic laboratory results we will use the EPA lab to state software.
2. There is no database.
3. Oracle Database Tomcat web application Server.
4. Java, using Tomcat and EPA supplied war file.

14. Is WV using the EPA SDWIS/State application or their own? If WV is using their own version what type of database does SDWIS/State have? What is the technology(s) used in the SDWIS/State software? Is the SDWIS/State database accessible?

1. **Response:** WV uses EPA SDWIS/State application
2. Not applicable.
3. Oracle Database, Tomcat web application server
4. Yes SDWIS/State is available behind our firewall. Successful bidder will either send us the files/ code to upload, come onsite to help install, or have a VPN connection provided to them.

15. What percentage of the SDWIS flow that must be implemented in the new manual data entry interface? Does the whole schema need to be represented or are the required elements enough to satisfy this task?

Response:

1. 100% of the SDWIS flow must be implemented in the new manual data entry interface.
2. The whole schema needs to be represented.

16 Does SDWIS/State application need to be modified?

Response: The SDWIS/State application does not need to be modified.

17. Does the Lab to State for Laboratories application need to be modified?

Response: WV does not believe that the application will need to be modified. However, there is the potential that there might be a need in conjunction with those laboratories that do not have LIMS (Laboratory Information Management Systems) and must use the manual interface.

18. Who are the parties that need to exchange this data (Lab to State) and what will be the direction of the flow?

Response: All WV Certified Drinking Water Laboratories have the potential of sending WV data. A current listing of these labs can be found at:
<http://www.wvdhhr.org/labservices/shared/docs/EnvMicro/waterqualitylabs.pdf>

Generally, the direction of flow will be from the laboratory to the State. CROMERR requirements has some correspondence that must be sent from the State to the sending party for verification that the submission was not altered during transmission and that the submission was sent from an authorized person.

19. Will the flow need only to import data into SDWIS/State, or will data need to be exported out of SDWIS/State also using the SDWIS exchange schema?

Response: The flow for Deliverable Number 2 will only import data into SDWIS/State.

20. Is the current WV SDWIS data flow CROMERR compliant?

Response: There is no current WV SDWIS data flow.

21. Has WV gone through the necessary CROMERR conformance planning exercise, such as development of the checklist and other items? If so can those be made available?

Response: Yes. A preliminary CROMERR checklist and other items has been performed, using the EPA Lab to State checklist as the starting point. WV has not submitted a privacy application to EPA as of this date.

22. What is a WV DHHR Monthly Operational Report and how many data entry elements does it contain? Can WV provide a mock-up or example of the monthly operational reports?

Response: The WVDHHR Monthly Operational reports are documents that are submitted from Public Water Systems each month and identify items such as; hours of pumping, amount of water treated, type and amount of chemicals used in the treatment process, chlorine residual, sampler identification, pH along with other items. There are various versions dependent on the source water type and the data elements are also different as per the version. The blank forms are located as follows:
<http://www.wvdhhr.org/oehs/eed/c&e/mor.asp> . Attached are completed versions of the forms.

23. Is there a data flow schema already created for the transfer of the above report or does one need to be created as well?

Response: No information is currently being submitted electronically, therefore, a schema will need to be created.

24. Who are the parties that need to exchange this data and what will be the direction of the flow?

Response: Potentially, if all the public water systems were to submit the Monthly Operational Reports electronically, there is the potential of 1,307 parties submitting data that needs to be imported through the Node to SDWIS/State.

25. Will the new flow be used only to import data, or will exporting data be needed as well?

Response: The flow for Deliverable Number 3 will only import data into SDWIS/State.

26. Have any additional requirements been developed for this deliverable (#4) and if so can they be made available to the vendor.

Response: No additional requirements have been developed.

27. Will this new system be used only to view data, or will it also be used to make edits and create new records?

Response: The system will be used to view data only, it will not be used to make edits and create new records.

28. How many data elements from SWOCS/SDWIS will be available to view with this system?

Response: A minimum of four data elements: certification held, date of issue, date of expiration, and CEH's credited. There could be multiple CEH records per individual.

29. Will there be various level of access based on user types/roles and what each of the user type will see/able to do within the system?

Response: Only one level of access is envisioned. The user should only be able to view their individual data.

30. Is SWOCS the same system as SDWIS/State or a different one and, if different, what technology(s) and database are behind the system?

Response: SWOCS is an "add-on" software that is linked to SDWIS/State, but has additional tables. The technology is Java and the Database is Oracle.

31. What is WV DHHR's preferred technical platform for deployment of the Node and development of associated applications?

Response: JAVA and Oracle 10g DB, and Oracle Application Server 10g are the preferred deployments for the Node and associated applications.

32. Page 5 indicates that the vendor must "Develop and implement a Web-based Electronic Data Interchange (EDI) on the Node". Please describe this EDI process and the data to be transferred.

Response: The vendor must install the Node to implement Lab to State, which is an EDI process, and develop a means for water systems to send Monthly Operational Report data to WV through the Node.

33. It is assumed that the PWS's will be able to submit all 4 monthly operating reports through the Web interface. Is this correct?

Response: Yes

34. Does WV DHHR have SWOCS running locally?

Response: WV DHHR has SWOCS running locally.

35. On Page 5 it states "Develop Safe Water Operator Certification System (SWOCS) web site from the SWOCS dataflow created on the node". But the deliverables on page 6 do not mention the need for a SWOCS dataflow. Please describe this data flow requirement.

Response: There is no data flow requirement for SWOCS.

36. Which other databases may be utilized to display data for this inquiry application (deliverable 4)?

Response: There would be no other data bases necessary to display data for this inquiry application.

37. The scope of work does not specify any qualifications other than Section IV. Vendor Agreement. However, the statement says, "vendor agrees to meet all requirements stated below upon successful quotation acceptance." This is a pretty basic list of requirements and really does not demonstrate technical capability of vendors. Part C of Section IV is only a rudimentary summary of past experience. It appears that this contract will be simply awarded to the lowest bidder without regard to technical capabilities. Is this RFQ at least Best Value, where the state would be able to use qualifications and pricing together in making the award decision? How does the state plan on determining technical capabilities of each firm other than Part C of Section IV?

Response: This is an RFQ and it is based on the lowest bidder meeting specifications, as written in the RFQ. The low bidder will need to meet the necessary requirements to be a vendor to the state.

38. Would it be more beneficial to the state to do a "Best Value" RFQ, including a statement of qualifications?

Response: This is an RFQ and the successful bidder will be based on the lowest bid meeting specifications, as written in the RFQ.

EW-210

AUG 08 2009

MONTHLY OPERATIONAL REPORT
Purchasers

PWSID Number: WV 3301814 Month/Year: July 2009
SYSTEM NAME: Northern Jackson County Public Service District PHONE NUMBER: 273-9621 COUNTY: Jackson
SYSTEM WATER IS PURCHASED FROM: RAVENSWOOD, WV COUNTY: Jackson

DATE	SYSTEM CHLORINE RESIDUAL (Total)	SAMPLING LOCATION FOR CHLORINE RESIDUAL	SAMPLER INITIALS	CHLORINE ADDED* (LBS or GAL)	METER READING (Gal)**	WATER PURCHASED (Gal)**
INITIAL METER READING:					525107000	
1	0.6	NJCPSD	mf		525243000	-136000
2	0.6	NJCPSD	mf		525375000	-132000
3	0.8	R Angus	ra		525506000	-131000
4	0.8	R Angus	ra		525638000	-132000
5	0.9	R Angus	ra		525769000	-131000
6	0.5	NJCPSD	mf		525930000	-181000
7	0.8	Brierwood 21 Booster	ra		526075000	-145000
7	0.7	Drift Run 04 765	ra		526075000	0
7	0.5	McGraw Run Rd Booster	ra		526075000	0
8	0.6	NJCPSD	mf		526212000	-137000
9	0.7	NJCPSD	mf		526355000	-143000
10	0.7	NJCPSD	mf		526485000	-130000
11	0.8	J Hickman	jh		526632000	-147000
12	0.8	J Hickman	jh		526779000	-147000
13	0.7	NJCPSD	mf		526938000	-159000
14	0.7	NJCPSD	mf		527087000	-149000
15	0.7	NJCPSD	mf		527230000	-143000
16	0.8	NJCPSD	mf		527367000	-137000
17	0.6	NJCPSD	mf		527501000	-134000
18	0.8	R Angus	ra		527638000	-137000
19	0.8	R Angus	ra		527778000	-138000
20	0.6	NJCPSD	mf		527917000	-141000
21	0.8	NJCPSD	mf		528061000	-144000
22	0.8	NJCPSD	mf		528214000	-153000
23	0.8	NJCPSD	jh		528352000	-138000
24	0.7	NJCPSD	mf		528493000	-141000
25	0.8	J Hickman	jh		528606000	-113000
26	0.7	J Hickman	jh		528720000	-114000
27	0.5	NJCPSD	mf		528873000	-153000
28	0.7	NJCPSD	mf		529015000	-142000
29	0.7	NJCPSD	mf		529141000	-126000
30	0.8	NJCPSD	mf		529277000	-136000
31	0.7	NJCPSD	mf		529431000	-154000
						0
						0
Total	23.5					
Average	0.8	AVERAGE				-4324000
Highest Reading	0.9					
Lowest Reading	0.5					

* Type of Chlorine Used: ___ Gas ___ Sodium Hypochlorite ___ Calcium Hypochlorite ___ None Added
** Optional Information

Water Purchased for the Month: 4,324,000 Gallons

I certify the values recorded above are true and accurate to the best of my knowledge.

CERTIFIED BY: Margie Flinn

CERTIFIED BY: *Margie Flinn*
(Certified Operator Signature required)

Certification #: 2011012305

Certification Exp. Date: 04/11/2011

Certification Class: 1

Complete and return within 10 calendar days after the end of the month to:
WV Office of Environmental Health Services - Date Management
Capitol & Washington Streets, 1 Davis Square, Suite 200
Charleston, WV 25301-4788
Phone: (304) 658-2981 FAX: (304) 658-0139

MONTHLY OPERATIONAL REPORT

Groundwater

PWSID NUMBER: WV 3301804

MONTH/YEAR: AUG 06 2009
July 2009

SYSTEM NAME: CoHagevi, 110 Pub. Serv. Dist. PHONE NUMBER: (304) 372-4317 COUNTY: JACKSON

DATE	TOTAL Time Pumped (hrs)	TOTAL Water Treated (GAL)	CHEMICALS USED		ANALYTICAL RESULTS (No. 2)						
			Chlorine <input type="checkbox"/> Gas <input type="checkbox"/> Dry (lb) <input type="checkbox"/> Liquid (oz)	Corrosion Control (lbs) **	Chlorine Residual		Sampling Location for Total Chlorine Residual	Samples In/Out	Alkalinity or Corrosion Control Residual **	pH	
					Plant Free	System Total				Raw *	Treated
7/1/09	12.9 hrs	257,600	1.03 lb		1.03	.64	Cottagesville	JH	262	7.11	7.08
7/2/09	16.4 hrs	256,500	1.31 lb	N/A	1.02	.64	Cottagesville	JH	265	7.11	7.09
7/3/09	16 hrs	260,800	1.28 lb		1.03	.63	Cottagesville	JH	255	7.12	7.08
7/4/09	14.6 hrs	239,200	1.16 lb		1.03	.63	Cottagesville	JH	255	7.10	7.07
7/5/09	17.6 hrs	288,100	1.40 lb		1.02	.60	Cottagesville	JH	258	7.11	7.07
7/6/09	16.6 hrs	268,900	1.32 lb		1.02	.61	Cottagesville	JH	260	7.10	7.08
7/7/09	17.3 hrs	278,600	1.38 lb		1.03	.62	Cottagesville	JH	258	7.10	7.07
7/8/09	17 hrs	277,500	1.36 lb		1.03	.63	Cottagesville	JH	262	7.11	7.07
7/9/09	16.7 hrs	301,600	1.33 lb		1.02	.62	Cottagesville	JH	260	7.11	7.08
7/10/09	16.8 hrs	280,000	1.34 lb		1.02	.63	Cottagesville	JH	255	7.12	7.09
7/11/09	16.4 hrs	271,900	1.31 lb		1.01	.61	Cottagesville	JH	255	7.10	7.08
7/12/09	17.2 hrs	279,900	1.37 lb		1.02	.61	Cottagesville	JH	262	7.12	7.09
7/13/09	16.2 hrs	269,300	1.29 lb		1.01	.62	Cottagesville	JH	262	7.12	7.09
7/14/09	20.9 hrs	337,400	1.67 lb		1.03	.63	Cottagesville	JH	255	7.10	7.07
7/15/09	15 hrs	246,800	1.20 lb		1.03	.65	Millwood	JH	255	7.10	7.07
7/16/09	17.4 hrs	281,600	1.39 lb		1.02	.64	Millwood	JH	262	7.11	7.08
7/17/09	14.7 hrs	248,600	1.17 lb		1.02	.66	Millwood	JH	260	7.11	7.08
7/18/09	17.4 hrs	289,900	1.39 lb		1.03	.64	Millwood	JH	262	7.10	7.08
7/19/09	18.4 hrs	310,800	1.47 lb		1.01	.65	Millwood	JH	265	7.10	7.07
7/20/09	16.1 hrs	279,400	1.28 lb		1.03	.65	Millwood	JH	265	7.10	7.07
7/21/09	19.7 hrs	320,300	1.57 lb		1.02	.66	Millwood	JH	255	7.12	7.09
7/22/09	17.1 hrs	287,800	1.36 lb		1.03	.64	Millwood	JH	262	7.12	7.09
7/23/09	18.8 hrs	286,100	1.50 lb		1.02	.65	Millwood	JH	255	7.11	7.08
7/24/09	18 hrs	311,900	1.44 lb		1.01	.64	Millwood	JH	255	7.11	7.08
7/25/09	18.5 hrs	305,200	1.48 lb		1.03	.66	Millwood	JH	265	7.10	7.07
7/26/09	16 hrs	277,000	1.28 lb		1.02	.65	Millwood	JH	262	7.10	7.07
7/27/09	19 hrs	281,000	1.52 lb		1.03	.65	Millwood	JH	265	7.12	7.09
7/28/09	16.8 hrs	268,800	1.34 lb		1.02	.66	Millwood	JH	255	7.12	7.09
7/29/09	15.4 hrs	245,200	1.23 lb		1.02	.64	Millwood	JH	255	7.10	7.07
7/30/09	16.4 hrs	261,900	1.31 lb		1.01	.63	Millwood	JH	258	7.10	7.07
7/31/09	15.5 hrs	249,400	1.24 lb		1.02	.65	Millwood	JH	255	7.11	7.08
TOTAL	511.8 hrs	8,519,400			31.69	19.74			8,035	220.3	219.4
AVERAGE	16.5 hrs	274,819			1.02	.63			259	7.10	7.07
HIGHEST READING	20.9 hrs	337,400	1.67 lb	✓	1.03	.66			265	7.12	7.09
LOWEST READING	12.9 hrs	239,200	1.03 lb		1.01	.60			255	7.10	7.07

*RAW pH is an optional measurement. ** Required only if adding a corrosion control chemical (e.g. ash, caustic soda, Aquasorb).

I certify the values recorded above are true and accurate to the best of my knowledge.

CERTIFIED BY: JACK HOLCOMB
(Printed Certified Operator Name Required)
Jack Holcomb
(Certified Operator Signature Required)

Certification #: 2009003600 Expiration Date: 11/30/09 Certification Class: I

Complete and return within 10 days after the end of the month to:
WV Office of Environmental Health Services - Data Management
Capitol and Washington Streets, 1 Davis Square, Suite 200, Charleston, WV 25301-1798
Phone: (304) 558-2961 FAX: (304) 558-0139

EW-103

Revised 02/08

AUG 06 2009

PWSID NUMBER: WV 3301804

MONTH/YEAR: July 2009

INDIVIDUAL WELL PUMPING LOG

(Timed Pumped in Hours)

Date	Well #1	Well #2	Well #3	Well #4	Well #5	TOTAL
1 7/1/09	12.5 hrs.	1.2 hrs.				
2 7/2/09	12.6 hrs	1 hrs.				
3 7/3/09	9.1 hrs.	4.8 hrs.				
4 7/4/09	7.1 hrs.	5.5 hrs.				
5 7/5/09	8.2 hrs	6.8 hrs.				
6 7/6/09	13.3 hrs.	1.1 hrs.				
7 7/7/09	9.1 hrs.	5.5 hrs.				
8 7/8/09	9.1 hrs.	5.7 hrs.				
9 7/9/09	18.3 hrs.	7.4 hrs				
10 7/10/09	7.3 hrs.	8.6 hrs.				
11 7/11/09	13 hrs.	1.5 hrs.				
12 7/12/09	8 hrs.	6.7 hrs.				
13 7/13/09	11.2 hrs	3.1 hrs.				
14 7/14/09	16.3 hrs.	1.7 hrs.				
15 7/15/09	10.6 hrs.	2.8 hrs.				
16 7/16/09	12.4 hrs.	2.5 hrs.				
17 7/17/09	13.5 hrs	0				
18 7/18/09	1.3 hrs.	2.4 hrs.				
19 7/19/09	14.5 hrs.	2.2 hrs.				
20 7/20/09	13.4 hrs.	1.6 hrs.				
21 7/21/09	14.2 hrs.	2.8 hrs.				
22 7/22/09	15.5 hrs	0				
23 7/23/09	14.8 hrs.	1.6 hrs.				
24 7/24/09	11.4 hrs.	3.7 hrs.				
25 7/25/09	14.6 hrs	3.6 hrs.				
26 7/26/09	5 hrs.	9.9 hrs.				
27 7/27/09	11.5 hrs.	3.5 hrs.				
28 7/28/09	12.6 hrs.	1.7 hrs.				
29 7/29/09	11.9 hrs.	1.2 hrs.				
30 7/30/09	8.9 hrs.	5 hrs.				
31 7/31/09	10 hrs.	3.3 hrs.				
Average Capacity (gpm)	11.4 hrs. (300 gpm)	3.5 hrs. (300 gpm)				

REMARKS:

**FLUORIDATION REPORT
MONTHLY SUMMARY OF OPERATION**

PWSID NUMBER: **WV**

3303808
(Required)

MONTH/YEAR: **August 2009**

SYSTEM TYPE:(Mark One)

Ground Surface Ground Water Under the Influence of Surface Water

SYSTEM NAME **KINGWOOD WATER WORKS**

PHONE NUMBER **329-2350**

COUNTY **PRESTON**

FLUORIDE CHEMICAL USED: **SODIUM FLUORIDE**

PURITY: **98.6%**

DATE	GALLONS OF WATER TREATED*	POUNDS/GAL OF CHEMICALS USED	ANALYTICAL RESULTS (mg/L)	
			PLANT EFFLUENT	DISTRIBUTION SYSTEM
1	636,100	43.0	1.10	0.96
2	645,900	39.0	1.03	1.11
3	716,100	54.0	0.97	0.84
4	622,900	41.0	0.99	0.91
5	763,700	58.0	1.25	0.9
6	651,700	41.0	1.14	1.17
7	899,600	44.0	1.16	1.11
8	766,100	48.0	1.13	1.05
9	711,700	57.0	1.08	1.23
10	749,800	48.0	1.14	1.13
11	632,300	38.0	0.90	1.06
12	672,800	44.0	1.00	1.2
13	762,000	48.0	1.18	1.2
14	682,500	54.0	1.08	1.32
15	695,600	35.0	0.82	1.19
16	671,600	39.0	1.21	1.07
17	697,100	43.0	1.28	0.96
18	782,900	48.0	1.18	1.19
19	695,700	45.0	1.29	1.09
20	683,900	49.0	1.13	1.03
21	732,900	48.0	1.13	1.25
22	678,600	44.0	1.00	1.19
23	655,700	45.0	1.21	1.09
24	611,700	45.0	1.09	1.14
25	624,300	47.0	1.06	1.09
26	628,300	46.0	1.04	1.08
27	892,800	51.0	0.81	1.01
28	706,100	50.0	1.05	0.86
29	691,100	42.0	0.89	0.81
30	700,700	45.0	0.94	0.88
31	725,000	49.0	0.90	0.9
TOTAL	21,125,800	1,424.00	33.18	33.02
AVERAGE	681,477	45.94	1.07	1.07
HIGHEST READING			1.29	1.32
LOWEST READING			0.81	0.81

*Optional IF reported on EW-90/EW-103

I certify the values recorded above are true and accurate to the best of my knowledge.

CERTIFIED BY:

ROBERT MCVICKER
(Certified Operator Printed Name Required)
Robert McVicker
(Certified Operator Signature Required)

DATE: **9/9/09**

Certification#: **2010005190** Exp. Date **8/1/10** Certification Class **III**

Complete and return within 10 days after the end of the month to:
WV Office of Environmental Health Services - Data Management
Capitol and Washington Streets, 1 Davis Square, Suite 200, Charleston, WV 25301-1788
Phone: (304) 558-9711 FAX: (304) 558-0139

MONTHLY OPERATIONAL REPORT -Filter Plants
Required Surface((GWUDI))

JUL 02 2009

MONTH/YEAR: June 2009

PWSID NUMBER: WV 3300101

SYSTEM NAME: Belington Water Works

PHONE NUMBER: 823-2271

COUNTY: Barbour

DATE	Plant Oper Time	Filtered Water	Flow Rate (GPM)	CHEMICALS USED										Sodium Hydroxide lbs	ppm	Indicate chemicals used in blocks below										Number of Filters	Wash Water GALS
				DelpAC		Klaron		Cellquest		Fluoride (Net)		PAC				Pre Chlorine		Post Chlorine									
				ppm	ppm	lbs	ppm	lbs	ppm	lbs	ppm	ppm	ppm	ppm	ppm	ppm	ppm	ppm	ppm	ppm	ppm	ppm					
1	6.0	245800	683	38.0	18.5	85.0	41.5	0.8	0.4	4.0	2.0	12.8	1.1	0.0	1.6	0.8	3.4	1.7									
2	5.6	228600	674	36.0	19.0	58.0	30.7	0.8	0.4	3.0	1.6	12.0	1.2	0.0	1.4	0.7	3.0	1.6									
3	5.6	227300	676	38.0	20.0	60.0	31.7	0.8	0.4	3.0	1.6	10.5	1.0	0.0	1.6	0.8	2.8	1.5									
4	5.1	207500	678	34.0	19.6	70.0	40.4	0.8	0.5	3.0	1.7	12.3	1.3	0.0	1.8	1.0	3.4	2.0									
5	5.9	241100	681	40.0	19.9	58.0	28.8	0.9	0.4	3.0	1.5	12.0	1.1	0.0	2.0	1.0	3.4	1.7									
6	5.3	212300	688	32.0	18.1	51.0	28.8	0.9	0.5	3.0	1.7	9.8	1.0	0.0	1.2	0.7	2.8	1.6									
7	5.3	213300	671	32.0	18.0	52.0	29.2	0.8	0.4	3.0	1.7	9.9	1.0	0.0	1.2	0.6	3.0	1.6									
8	5.6	228300	685	40.0	21.5	88.0	35.4	0.8	0.5	3.0	1.6	12.3	1.2	0.0	1.2	0.6	3.0	1.6									
9	5.6	226800	675	38.0	19.0	58.0	29.6	0.7	0.4	3.0	1.6	9.8	0.9	0.0	1.4	0.7	2.8	1.5									
10	3.9	157800	674	26.0	19.8	37.0	28.2	0.6	0.5	2.0	1.5	6.2	0.9	0.0	1.0	0.8	2.6	2.0									
11	6.8	277500	680	46.0	19.9	49.0	21.2	1.1	0.5	4.0	1.7	13.0	1.0	0.0	1.8	0.8	3.4	1.5									
12	5.7	227900	686	38.0	20.0	47.0	24.7	1.0	0.5	3.0	1.6	12.2	1.2	0.0	1.6	0.8	3.4	1.8									
13	5.2	209500	671	28.0	16.0	32.0	18.3	0.7	0.4	3.0	1.7	9.1	0.9	0.0	1.0	0.6	3.0	1.7									
14	5.3	215200	677	32.0	17.8	40.0	22.3	0.7	0.4	3.0	1.7	11.4	1.2	0.0	1.2	0.7	3.4	1.9									
15	6.2	250900	674	42.0	20.1	48.0	22.9	1.0	0.5	3.0	1.4	10.7	0.9	0.0	2.0	1.0	3.6	1.7									
16	5.6	228500	680	34.0	17.8	36.0	18.9	0.8	0.4	3.0	1.6	9.5	0.9	0.0	1.4	0.7	2.8	1.5									
17	5.2	210900	676	34.0	19.3	40.0	22.7	0.8	0.5	3.0	1.7	10.5	1.1	0.0	1.4	0.8	2.8	1.6									
18	5.5	223200	675	38.0	20.4	43.0	23.1	1.0	0.5	3.0	1.6	10.4	1.0	0.0	1.6	0.9	3.2	1.7									
19	6.2	249300	670	42.0	20.2	41.0	19.7	1.0	0.5	3.0	1.4	12.1	1.1	0.0	1.8	0.9	3.4	1.6									
20	5.3	218400	687	36.0	19.8	38.0	20.9	0.8	0.4	3.0	1.6	10.0	1.0	0.0	1.4	0.8	3.0	1.6									
21	5.8	232800	669	38.0	19.6	41.0	21.1	0.9	0.5	3.0	1.5	10.2	1.0	0.0	1.6	0.8	3.0	1.5									
22	5.1	208500	681	32.0	18.4	38.0	21.9	0.9	0.5	3.0	1.7	11.1	1.2	0.0	1.6	0.9	2.6	1.6									
23	5.4	216500	688	28.0	15.5	37.0	20.5	0.9	0.5	3.0	1.7	9.8	1.0	0.0	1.8	0.9	2.8	1.6									
24	6.2	249100	670	38.0	18.3	48.0	23.1	1.1	0.5	4.0	1.9	12.3	1.1	0.0	1.8	0.9	3.4	1.6									
25	5.6	225200	670	36.0	19.2	44.0	23.4	1.0	0.5	3.0	1.6	10.8	1.0	0.0	1.8	0.9	3.4	1.6									
26	5.5	226500	686	36.0	19.1	38.0	20.1	0.8	0.4	3.0	1.6	9.9	1.0	0.0	1.6	0.8	3.2	1.7									
27	5.5	224200	679	38.0	20.3	40.0	21.4	0.9	0.5	3.0	1.6	9.8	1.0	0.0	1.8	1.0	3.0	1.6									
28	6.5	226700	687	38.0	20.1	38.0	20.1	0.9	0.5	3.0	1.6	10.2	1.0	0.0	1.8	1.0	3.2	1.7									
29	6.2	249600	671	44.0	21.1	48.0	22.1	1.1	0.5	4.0	1.9	12.4	1.1	0.0	2.2	1.1	3.8	1.8									
30	4.5	189900	688	30.0	19.4	30.0	19.4	0.8	0.5	3.0	1.9	9.1	1.1	0.0	1.6	1.0	3.0	1.9									
31																											
TOTAL	166.2	6737900	20273	1090.0	575.8	1407.0	752.1	28.2	14.0	93.0	49.6	322.2	31.3		48.8	24.9	98.2	49.9									
AVG	5.6	224597	676	36.0	19.2	46.9	25.1	0.9	0.5	3.1	1.7	10.7	1.0		1.6	0.8	3.1	1.7									

JUL 02 2009

PWSID NUMBER: WV 3300101


MONTH/YEAR: June 2009

MONTHLY OPERATIONAL REPORT REMARKS

Date	Plant (Frate)	System (Total)	Sampling Location of System Total Chlorine Residual	Sampler Initials	Chlorine Residual (mg/L)			Turbidity (NTU)			pH (S.U.)			MONTHLY OPERATIONAL REPORT REMARKS
					Raw	Settled	Finished	Raw	Settled	Finished	Raw	Settled	Finished	
1	1.51	1.2	Fire House	D.H.	20.98	0.78	0.05	7.51	7.51	7.98				
2	1.34	0.9	D.O.H. Garage	D.H.	5.75	0.64	0.06	7.66	7.53	7.91				
3	1.31	0.6	Stevens Supply	D.H.	9.50	0.53	0.05	7.71	7.49	7.94				
4	1.23	1.0	Exxon Station	D.H.	5.52	0.97	0.04	7.88	7.56	7.97				
5	1.48	1.2	Waste Water Plant	D.H.	30.70	0.87	0.05	7.63	7.52	7.91				
6	1.35	0.7	Civic Center	D.H.	13.66	0.88	0.03	7.38	7.23	7.83				
7	1.33	0.9	City Garage	D.H.	7.05	0.77	0.04	7.55	7.44	7.87				
8	1.22	0.9	City Park	D.H.	4.81	0.86	0.11	7.86	7.43	7.94				
9	1.62	1.0	Fire House	D.H.	4.08	0.48	0.04	7.81	7.47	7.89				
10	1.40	0.7	D.O.H. Garage	D.H.	6.73	0.57	0.05	7.59	7.38	7.86				
11	1.30	0.8	Stevens Supply	D.H.	3.20	0.48	0.04	7.61	7.41	7.79				
12	1.38	1.2	Exxon Station	D.H.	1.89	0.49	0.03	7.66	7.41	8.02				
13	1.25	1.2	Waste Water Plant	D.H.	2.40	0.41	0.06	7.61	7.44	7.92				
14	1.21	0.8	Civic Center	D.H.	1.76	0.82	0.04	7.72	7.53	7.96				
15	1.30	0.7	City Garage	D.H.	1.90	0.68	0.04	7.72	7.61	7.98				
16	1.31	0.8	City Park	D.H.	1.88	0.62	0.04	7.58	7.35	7.91				
17	1.15	1.0	Fire House	D.H.	2.36	0.19	0.07	7.73	7.35	7.90				
18	1.30	0.5	D.O.H. Garage	D.H.	1.41	0.51	0.05	7.61	7.45	7.95				
19	1.18	0.7	Stevens Supply	D.H.	1.70	0.66	0.04	7.66	7.49	7.97				
20	1.04	0.9	Exxon Station	D.H.	1.77	0.55	0.03	7.55	7.45	8.00				
21	0.99	1.3	Waste Water Plant	D.H.	3.81	0.62	0.08	7.61	7.51	7.92				
22	1.08	0.8	Civic Center	D.H.	3.73	0.97	0.05	7.64	7.46	7.88				
23	1.28	0.9	City Garage	D.H.	5.94	0.84	0.05	7.59	7.33	7.95				
24	1.02	0.5	City Park	D.H.	1.34	0.75	0.04	7.89	7.52	7.97				
25	1.13	1.2	Fire House	D.H.	2.00	0.65	0.09	7.59	7.46	7.94				
26	1.08	0.9	D.O.H. Garage	D.H.	3.08	0.43	0.04	7.73	7.48	7.90				
27	1.10	0.9	Stevens Supply	D.H.	1.55	0.51	0.04	7.68	7.44	7.92				
28	1.04	1.1	Exxon Station	D.H.	0.88	0.49	0.04	7.62	7.39	7.88				
29	1.11	1.1	Waste Water Plant	D.H.	0.96	0.45	0.03	7.66	7.46	7.90				
30	1.05	0.7	Civic Center	D.H.	0.91	0.69	0.04	7.68	7.56	7.93				
31														
TOTAL	37.07	27.0			153.33	18.98	1.41	229.02	223.82	237.69				
AVG	1.24	0.9			5.11	0.63	0.05	7.53	7.46	7.92				

I certify the values recorded above are true and accurate to the best of my knowledge.

Certified by:

Donald Harris
 (Certified Operator Printed Name Required)

 (Certified Operator Signature Required)

Date:

07/01/09

Certification #:

2010003280 Exp. Date: 12/31/10

Certification Class

II

Number of Filters Used: 2
 Total Filter Surface Area: 150 (sq. ft.)
 Average Filter Run/Each Filter: 17 (hrs.)
 % Backwash Water: 3.31%

Complete and return within 10 days after the end of the month to:
 WV Office of Environmental Health Services - Data Management
 Capitol and Washington Streets, 1 Davis Square, Suite 200, Charleston, WV 25301-1798
 Phone: (304) 558-6711 FAX: (304) 558-0139

THIS PAGE IS OPTIONAL

JUL 02 2009

PWSID NUMBER: WV

3300101

MONTH/YEAR:

June 2009

ANALYTICAL RESULTS (mg/L)

DATE	Iron		Manganese		Phenolphthalein Alkalinity		Total Alkalinity		Calcium Hardness		Total Dissolved Solids (TDS) Finished	TEMP °F or C° (Finished)	Langlier Saturated Index (Finished)
	Raw	Finished	Raw	Finished	Raw	Finished	Raw	Finished	Raw	Finished			
1							20	26					
2							22	28					
3							24	28					
4							24	30					
5							22	28					
6	0.42	0.01	0.056	0.02			24	28	27		69.7	22	-1.16
7							22	26					
8							22	26					
9							24	28					
10							22	26					
11							24	30					
12							22	26					
13	0.36	0.01	0.044	0.018			24	28	26.6		72.2	23	-1.02
14							22	28					
15							24	30					
16							24	28					
17							22	28					
18							22	26					
19							24	28					
20	0.24	0	0.053	0.008			28	32	34.5		78.2	23.6	-0.8
21							24	28					
22							22	28					
23							24	30					
24							26	32					
25							24	32					
26							26	34					
27							28	34					
28	0.32	0.02	0.066	0.012			26	32	32.2		66.6	22.8	-0.96
29							28	34					
30							26	34					
31													
TOTAL	1.34	0.04	0.221	0.058			716	878	120.3		286.7	91.4	-3.94
AVG	0	0	0.055	0			24	29	30		72	23	-1

JUL 02 2009

INDIVIDUAL FILTERS

If method is other than direct or conventional, please specify
(Please note, direct and /or conventional methods are required to complete the form below)

_____ (diatomaceous earth, slow sand, other)

1. Was each filter monitored continuously?

Yes No

2. Were measurements recorded every 15 minutes?

Yes No

3. Was there a failure of continuously turbidity monitoring equipment?

Yes No

4. Were individual filter levels greater than 1.0 NTU in two consecutive measurements?

Yes No

5. Were individual filter levels greater than 0.5 NTU in two consecutive measurements after online for more than four hours?

Yes No

6. Were individual filter levels greater than 1.0 NTU in two consecutive measurements in three consecutive months?

Yes No

7. Were individual filter levels greater than 2.0 NTU in two consecutive measurements in two consecutive months?

Yes No

FILTER NUMBER	
TURBIDITY MEASUREMENTS	
DATE(S) AND TIME(S)	

I certify the information recorded above is true and accurate to the best of my knowledge.

CERTIFIED BY: Donald Harris
Operator Printed Name required

CERTIFIED BY: *Donald Harris*
Operator Signature required

Date: 07/01/09

Certification # 2010003280 Exp. Date 12/31/10 Certification Class II

MONTHLY COMBINED FILTER EFFLUENT TURBIDITY REPORT
 Required Surface/GWUDI Systems

PWSID NUMBER: WV 3300101

MONTH/YEAR: June 2009

SYSTEM TYPE: (Check One) Surface

GWUDI

SYSTEM NAME:

Beilington Water Works

PHONE NUMBER

823-2271

COUNTY

Barbour

Please report NTU values to two decimal places (0.00)

DATE	TIME	NTU	TIME	NTU	TIME	NTU	TIME	NTU	TIME	NTU	#<=0.3	#>0.3	REMARKS
1	800	0.05	1100	0.03	1400	0.03					3		
2	800	0.06	1100	0.04	1400	0.03					3		
3	800	0.05	1100	0.04	1400	0.03					3		
4	800	0.04	1100	0.04	1400	0.03					3		
5	800	0.05	1400	0.05	1400	0.05					3		
6	800	0.03	1100	0.03	1400	0.03					3		
7	800	0.04	1100	0.04	1400	0.04					3		
8	800	0.11	1100	0.05	1400	0.03					3		
9	800	0.04	1100	0.03	1400	0.03					3		
10	800	0.05	1100	0.04	1400	0.04					3		
11	800	0.04	1100	0.04	1400	0.03					3		
12	800	0.03	1100	0.03	1400	0.03					3		
13	800	0.06	1100	0.05	1400	0.03					3		
14	800	0.03	1100	0.04	1400	0.04					3		
15	800	0.04	1100	0.04	1400	0.03					3		
16	800	0.04	1100	0.03	1400	0.03					3		
17	800	0.07	1100	0.07	1400	0.04					3		
18	800	0.06	1100	0.05	1400	0.04					3		
19	800	0.04	1100	0.03	1400	0.03					3		
20	800	0.03	1100	0.03	1400	0.03					3		
21	800	0.03	1100	0.03	1400	0.03					3		
22	800	0.05	1100	0.04	1400	0.04					3		
23	800	0.05	1100	0.04	1400	0.03					3		
24	800	0.04	1100	0.03	1400	0.03					3		
25	800	0.09	1100	0.06	1400	0.03					3		
26	800	0.03	1100	0.04	1400	0.04					3		
27	800	0.04	1100	0.03	1400	0.03					3		
28	800	0.04	1100	0.03	1400	0.04					3		
29	800	0.03	1100	0.03	1400	0.03					3		
30	800	0.03	1100	0.03	1400	0.04					3		
31	800		1100		1400						3		

GRAND TOTAL = **100%** Highest Single turbidity reading 0.110 Total # of Samples 90 Lowest Single turbidity reading 0.030

CERTIFIED BY: Donald Harris (Certified Operator Printed Name Required)
Donald Harris (Certified Operator Signature Required)
 Date: 07/01/09

Certification #: 2010003280 Exp. Date 12/31/10 Classification Class II
 Complete and return within 10 days after the end of the month to:
 WV Office of Environmental Health Services - Data Management
 Capitol and Washington Streets, 1 Davis Square, Suite 200, Charleston, WV 25301-1798
 Phone: (304) 558-6711 FAX: (304) 558-0139

JUL 02 2009

JUL 02 2009

EW-90B Revised 02/05

MONTHLY CHLORINE RESIDUAL REPORT - Required Surface and GWUDI Sources
Required for Surface/GWUDI Systems

PWSID NUMBER: WV 3300101

MONTH/YEAR: June 2009

SYSTEM TYPE:(Check One) Surface GWUDI

SYSTEM NAME Belington Water Works PHONE NUMBER 823-2271 COUNTY Barbour

Please report Chlorine Residual values to one decimal places (0.0)

DATE	TIME	CL. RES.	TIME	CL. RES.	TIME	CL. RES.	TIME	CL. RES.	TIME	CL. RES.	TIME	CL. RES.	TOTAL
1	800	1.55	1100	1.52	1400	1.51							3
2	800	1.34	1100	1.39	1400	1.37							3
3	800	1.31	1100	1.41	1400	1.37							3
4	800	1.23	1100	1.24	1400	1.42							3
5	800	1.49	1100	1.55	1400	1.48							3
6	800	1.37	1100	1.38	1400	1.35							3
7	800	1.33	1100	1.34	1400	1.38							3
8	800	1.22	1100	1.42	1400	1.5							3
9	800	1.63	1100	1.66	1400	1.62							3
10	800	1.45	1100	1.39	1400	1.4							3
11	800	1.3	1100	1.3	1400	1.49							3
12	800	1.4	1100	1.38	1400	1.41							3
13	800	1.37	1100	1.28	1400	1.25							3
14	800	1.21	1100	1.2	1400	1.31							3
15	800	1.3	1100	1.35	1400	1.37							3
16	800	1.31	1100	1.33	1400	1.32							3
17	800	1.15	1100	1.39	1400	1.44							3
18	800	1.3	1100	1.32	1400	1.33							3
19	800	1.18	1100	1.2	1400	1.3							3
20	800	1.05	1100	1.05	1400	1.04							3
21	800	0.99	1100	1.44	1400	1.37							3
22	800	1.06	1100	1.58	1400	1.6							3
23	800	1.28	1100	1.26	1400	1.29							3
24	800	1.02	1100	1.23	1400	1.18							3
25	800	1.13	1100	1.24	1400	1.29							3
26	800	1.08	1100	1.27	1400	1.36							3
27	800	1.1	1100	1.08	1400	1.21							3
28	800	1.04	1100	1.25	1400	1.26							3
29	800	1.11	1100	1.39	1400	1.38							3
30	800	1.06	1100	1.05	1400	1.35							3
31	800		1100		1400								3
												# of Samples under 0.2 mg/l (free chlorine residual) <u>0</u>	Total # of Samples Taken <u>90</u>

Max 1.66 Min 0.99 Avg. 1.313111

I certify the values recorded above are true and accurate to the best of my knowledge.

CERTIFIED BY:

Donald Harris

(Certified Operator Printed Name required)

Donald Harris
(Certified Operator Signature required)

Date: July 01, 2009

Certification #:

201003280

Exp. Date

December 31, 2010

Certification Class

II

Complete and return within 10 days after the end of the month to:
WV Office of Environmental Health Services - Data Management
Capitol and Washington Streets, 1 Davis Square, Suite 200, Charleston, WV 25301-1798
Phone: (304) 558-6711 FAX: (304) 558-0139

**QUARTERLY OPERATIONAL REPORT
DISINFECTION BYPRODUCT
PRECURSORS CONTROL**
(Conventional Filtration Only)

PWSID NUMBER: WV 3300806 QUARTER / YEAR 3rd 2009
(Required)

SYSTEM TYPE:
(Check One) Ground Surface Ground Water Under the Direct Influence of Surface Water

System Name Clay-Roane PSD (Precious District) County Clay

Treatment Plant Name Precious Plant

Month	Source Water		Treated Water TOC (mg/L)	(A) Actual % TOC Removal	(B) Required% TOC Removal	(C) Removal Ratio (A) / (B)	Basis for Required % Removal
	ALK (mg/L)	TOC (mg/L)					
August 2008	32.2	1.82	1.44	21%	35%	1.0	A2
September 2008	35.6	1.93	1.50	22%	35%	1.0	A2
October 2008	29.8	2.61	1.77	32%	35%	1.0	A2
November 2008	19.1	2.35	1.09	54%	35%	1.0	A2
December 2008	21.1	2.14	1.50	30%	35%	1.0	A2
January 2009	14.8	1.49	1.09	27%	35%	1.0	A2
February 2009	12.3	1.41	1.11	21%	35%	1.0	A2
March 2009	8.3	1.45	1.22	16%	35%	1.0	A2
April 2009	15.0	1.67	1.28	23%	35%	1.0	A2
May 2009	15.1	2.12	1.71	19%	35%	1.0	A2
June 2009	19.8	3.61	2.21	39%	35%	1.0	A2
July 2009	28.4	2.05	1.67	19%	35%	1.0	A2
Total	251.5	24.7	17.6	3.2	4.2	12.0	
Annual Average	21.0	2.1	1.5	0.3	0.4	1.0	

CERTIFIED BY: William Miller
(Certified Operator's Printed Name Required)


(Certified Operator's Signature Required)

Date: July 31, 2009

Certification # 2010007957 Expiration Date February 15, 2009

Certification Class 3 Telephone Number 304-548-5209

Complete and return within 10 days after the end of the quarter to:
WV Office of Environmental Health Services RD&C Unit
Capitol and Washington Streets, 1 Davis Square, Suite 200, Charleston, WV 25301-1798
Phone: (304) 558-6711 FAX: (304) 558-0139

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 1 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

1.0 PURPOSE

This policy defines and protects the integrity of the Department of Health and Human Resources (DHHR) network(s).

2.0 SCOPE

This policy applies to all DHHR employees accessing DHHR supported applications and computer systems. It also applies to personnel from other departments, agencies, contractors, and vendors using DHHR's data communications system(s) or networks which may be composed of any combination of Local Area Networks (LANs), or Wide Area Networks (WANs).

3.0 APPLICABLE DOCUMENTS/MATERIAL

Several DHHR regulations and state and federal laws affect the security of information processing resources, computer systems, computer software, and data files. They include the following:

- 3.1 DHHR IT Policy 0501 – Use of IT Resources
Section 4.0 and Appendices A and B
- 3.2 DHHR IT Policy 0502 – Virus Prevention, Detection, and Removal
- 3.3 DHHR IT Policy 0513 – Physical Security for IT Resources
- 3.4 DHHR IT Policy 0514 – Disaster Recovery
- 3.5 DHHR IT Policy 0518 – Access Authorization and Modification
- 3.6 Office of Management Information Services (OMIS) Operating Procedure (OP)-01
Computer Room Security/Access
- 3.7 All DHHR Employee and Vendor Confidentiality Statements
- 3.8 WV Code - §9-7-1, Confidentiality of Records
- 3.9 WV Computer Crime and Abuse Act - §61-3C-4 through 61-3C-21
- 3.10 WV Governor's Office of Technology (GOT) Directive
State of WV IT Information Security Policy
- 3.11 DHHR Common Chapters Manual

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 2 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

Chapter 200 – Confidentiality
Sections 1100-1150 – Computer Crimes

3.9 DHHR Policy Memorandum 2104 – Progressive Discipline

3.10 DHHR Policy Memorandum 2108 – Employee Conduct

3.11 Federal Computer Fraud and Abuse Act of 1996
 Us Code, Title 18, Chapter 47, Section 1030

3.12 Electronic Communications Privacy Act of 2000
 U.S. Code, Title 18, Chapter 119, Section 2511

4.0 RESPONSIBILITIES

4.1 Information Technology (IT) Asset Protection

4.1.1 The Chief Technology Officer (CTO) is responsible for the management, operation, and security of the DHHR network.

4.1.2 The CTO will ensure that IT assets are protected.

4.2 IT Network Security Management

4.2.1 A management committee will provide leadership on IT Network security matters in the DHHR.

4.2.2 The Information Security Officer (ISO) will coordinate IT security matters in the DHHR.

4.2.3 Periodic reviews will be conducted to verify compliance to the DHHR's network design, set-up, and configurations; as well as IT security policies and procedures.

4.2.4 Documentation of the IT security controls and procedures in the DHHR must be maintained.

4.3 User Security

4.3.1 All employees are required to comply with all applicable IT security policies and procedures.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 3 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

- 4.3.2 IT security responsibilities must be defined for relevant employees as part of their job scope.
- 4.3.3 An on-going awareness program must be established to educate and train all employees on DHHR IT security requirements.
- 4.3.4 All software and computing devices used to store, process, and access information related to the DHHR's functions and services must be identified and assessed for legitimacy.
- 4.3.5 Software applications must be updated promptly when security necessitated patches become available.
- 4.3.6 All employees must be educated on procedures regarding security.
- 4.3.7 Employees must be accountable for their computers and for any actions that can be identified to have originated from them.
 - 4.3.7.1 PC's must always be locked or logged-off when left unattended.
 - 4.3.7.2 Passwords must never be shared under any circumstances.
- 4.3.8 All programmable computing devices must contain virus protection software.
- 4.3.9 All network connections from computing devices must be uniquely identified and verified.
- 4.3.10 Computing devices will be subject to all DHHR security controls when connecting to the DHHR's internal network via remote access.
- 4.4 Vendor/Contractor Management
 - 4.4.1 Vendors/contractors will be subject to the same rules and regulations outlined in this policy.
 - 4.4.2 A risk assessment must be conducted to determine the security risks associated with giving a vendor and/or contractor access to a DHHR resource.
 - 4.4.3 Security requirements for vendors/contractors must be defined by DHHR and accepted by the vendor/contractor.
- 4.5 Resource Management

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 4 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

- 4.5.1 An owner must be defined for each IT resource.
- 4.5.2 The role-based access requirements of employees utilizing the IT resource must be defined.
- 4.5.3 All access to computing resources will be granted on a need-to-use basis.
- 4.5.4 Critical system software and files must be routinely backed-up.
- 4.6 Incident Management
 - 4.6.1 Incident response plans supporting the DHHR's security objectives must be established.
 - 4.6.2 Procedures, guidelines, and mechanisms that must be utilized during a security incident will be reviewed as needed.
 - 4.6.3 Roles and responsibilities of the incident management teams must be established and clearly defined.
- 4.7 Authentication
 - 4.7.1 All employees must be authenticated before they are given access to a resource intended for a restricted group.
 - 4.7.2 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.
- 4.8 Access Control
 - 4.8.1 Access to the DHHR's assets will be granted on a need-to-use basis.
 - 4.8.2 Access to assets must be approved by the resource owner or a designee.
 - 4.8.3 All access to any DHHR asset must be immediately disabled when access is no longer required.
- 4.9 Encryption Control
 - 4.9.1 Confidential or sensitive data (i.e., credit card numbers, calling card numbers, log-on passwords, etc.) must be encrypted before being transmitted through the Internet

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 5 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

- 4.9.2 All sensitive information requiring encryption protection must use an OMIS-approved cryptography system.
- 4.10 Database Security
- 4.10.1 Controls must be established and maintained in the management and administration of the databases. Appropriate authorization must be obtained for access and modification of databases.
- 4.11 Network Security
- 4.11.1 Access to network resources must be controlled and limited to authorized employees only.
- 4.11.2 The CTO or a designee will approve all network connections. The Network and Technical Support (NTS) group and/or the Data Center Desktop Support (DCDS) group will implement the appropriate access control mechanisms.
- 4.11.3 Networks spanning across the DHHR's boundaries will have defined multiple points, each protected by the appropriate security perimeter and access control mechanisms.
- 4.11.4 Applications accessible by the public must be placed in the demilitarized zone (DMZ).
- 4.11.5 The network access firewall and/or secure gateway must be configured to deny all incoming services unless explicitly permitted.
- 4.12 Network Monitoring and Compliance
- 4.12.1 NTS will monitor, oversee, and take actions to safeguard DHHR network traffic and network-based systems.
- 4.13 Security Operations
- 4.13.1 Only security tools authorized by the CTO or a designee must be used to enforce the IT security policies and procedures.
- 4.13.2 Security tools and any information derived from their use must be restricted and will be released as authorized by the CTO or a designee.
- 4.14 Availability, Recovery, and Business Continuity

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 6 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

- 4.14.1 Each Bureau/Office must work with OMIS to define the level of availability required to meet their business needs and service standards.
- 4.14.2 The DHHR must develop business continuity and recovery plans.
- 4.14.3 Employees involved in the business continuity and recovery plans must be aware of their roles and responsibilities during a disaster or a service disruption.
- 4.14.4 The business continuity and recovery plans must be tested periodically.
- 4.14.5 The DHHR must have documentation of its backup strategy.
- 4.14.6 Backups of critical business data and resources must be stored in an off-site physically secured environment.
- 4.15 Enforcement Authority
- 4.15.1 The ISO is the person designated by the CTO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
- 4.15.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.
- 4.15.3 The OIG (Office of the Inspector General) is the authority who investigates reported instances of departmental employee misconduct.
- 4.16 Violations and Disciplinary Action(s)
- 4.16.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.
- 4.16.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to the Office Director, Bureau Commissioner, or Community Services Manager (CSM) for appropriate action.
- 4.16.3 As determined by the Office Director or the Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 7 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

4.16.4 Employees who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

- 5.1 Access Control – rules for limiting access to safeguard systems and data at all times and under all conditions.
- 5.2 Chief Technology Officer (CTO) – The director of OMIS and the person responsible for all information resources within the DHHR.
- 5.3 Data Center Desktop Support (DCDS) – The OMIS organization that is responsible for the DHHR Data Center and the Kanawha County offices.
- 5.4 Demilitarized Zone (DMZ) – A network added between a protected network and an external network in order to provide an additional layer of security. (Sometimes called a perimeter network.)
- 5.5 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractors' employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.6 Encryption – The process of enciphering or encoding data so that it is inaccessible to unauthorized users.
- 5.7 Incident or Intrusion – An adverse event associated with an information system that: (1) fails to comply with security regulations or directives; (2) results in attempted or actual loss of data; (3) involves the waste, fraud, abuse, loss, or damage of property or information; and (4) reveals and/or exploits hardware or software vulnerabilities.
- 5.8 IT Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.
- 5.9 Local Area Networks (LAN) – A communications network made up of servers, workstations, a network operating system, and a communications link that serves employees within a confined geographical area.
- 5.10 Malicious Code – Computer instructions, usually in the form of a program, designed to perform undesired changes to the computer system, data, or programs. (Ex: computer virus)

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0511	REVISION: 01/02/04	PAGE 8 OF 8
SUBJECT: IT Network Security		EFFECTIVE DATE: 02/24/03	

- 5.11 Network – A system of computers, and often peripherals, such as printers, linked together. DHHR workstations are connected to a Wide Area Network (WAN), which is a larger network, which uses telephone lines or radio waves to link computers that can be up to thousands of miles apart.
- 5.12 Network Monitoring – Detection of break-ins or break-in attempts by reviewing logs or other information available on a network. Intrusion detection is essential for maintaining network security.
- 5.13 Network Monitoring Tools – Automated software tools that perform real-time analysis of data traffic, and employ advanced logic to detect patterns of activity that indicate that an intrusion attack is underway.
- 5.14 Network Security – Measures taken to protect a communications pathway from unauthorized access to, and accidental or willful interference of, regular operations.
- 5.15 Network Security Database – This will be established and maintained by the CIO. The purpose of the database is to maintain up-to-date contact information that will identify the emergency contact during a computer or network security incident, and for the dissemination of guidelines and procedures for network security.
- 5.16 Network and Technical Support (NTS) – The OMIS organization responsible for engineering and emerging technologies, Help Desk/Customer Support, and field support.
- 5.17 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
- 5.18 Resource/Data Owner – The person having primary responsibility for the creation and maintenance of the data content.
- 5.19 Risk Assessment – An evaluation of the following: (1) the exposure of an asset to the identified threats; (2) the potential impacts of an event; (3) an estimate of the likelihood of an event occurring; and (4) the effectiveness of existing or proposed safeguards to protect an asset.
- 5.20 Wide Area Network (WAN) – A communications network connecting computing devices over geographically distant locations. A WAN covers a much larger area than a LAN, such as a city, state, or country. WANs can either use phone lines or dedicated communication lines.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 1 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy establishes guidelines to protect information resources within the Department of Health and Human Resources (DHHR).

2.0 SCOPE

This policy applies to all DHHR employees who have access to, store data in, retrieve data from view, or otherwise make use of DHHR information resources.

3.0 APPLICABLE DOCUMENTS/MATERIAL

- 3.1 In instances where state and federal laws and regulations are more restrictive than DHHR IT policies, the more restrictive provisions will supersede.
- 3.2 DHHR IT Policy 0501 – Use of IT Resources
Appendix A – Employee Responsibilities
- 3.3 DHHR IT Policy 0510 – E-mail Guidelines and Requirements
- 3.4 DHHR IT Policy 0513 – Physical Security for IT Resources
- 3.5 DHHR IT Policy 0514 – Disaster Recovery
- 3.6 DHHR IT Policy 0518 – Access Authorization and Modification
- 3.7 OMIS Operating Procedure (OP) – 12 – E-mail
- 3.8 OMIS OP – 22 – Information Security Awareness Training
- 3.9 DHHR Employee and Vendor Confidentiality Statements
- 3.10 West Virginia Code – Section 49-7-1, Confidentiality of Records
- 3.11 West Virginia Computer Crime and Abuse Act – Section 61-3C-21

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 2 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 3.12 West Virginia Governors Office of Technology (WVGOT) Directive
State of West Virginia ITC Information Security Policy
- 3.13 DHHR Common Chapters Manual – Chapter 200, Confidentiality
- 3.14 DHHR Policy Memorandum 2104 – Progressive Discipline
- 3.15 DHHR Policy Memorandum 2108 – Employee Conduct
- 3.16 West Virginia Freedom of Information Act – WV Code, Chapter 29B
- 3.17 Federal Computer Fraud and Abuse Act of 1996
US Code, Title 18, Chapter 47, Section 1030
- 3.18 Electronic Communications Privacy Act of 2000
US Code, Title 18, Chapter 119, Section 2511
- 3.19 West Virginia Records Management and Preservation of Essential Records Act,
WV Code, Chapter 5A, Article 8
- 3.20 Health Insurance Portability and Accountability Act (HIPAA) of 1996
- 3.21 West Virginia Records Retention and Disposal Schedule for Department of Health

4.0 RESPONSIBILITY/REQUIREMENTS

4.1 Information Resources

- 4.1.1 Bureau Commissioners and their organizational equivalent(s) are responsible for the protection of information resources under their jurisdiction and control.
- 4.1.2 Information resources will be used only for intended purposes as defined by the Bureaus/Offices, will be consistent with applicable state and federal laws, and will satisfy all mandated federal compliance requirements.
- 4.1.3 All DHHR employees are accountable for their actions relating to information resources.
 - 4.1.3.1 Passwords must never be shared under any circumstances.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 3 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 4.1.4 The integrity of the data must be ensured (this includes its source, its destination, and the processes applied to it). Changes to data must only be made in authorized and acceptable ways.
- 4.1.5 Continuity of information resources supporting critical governmental services must be ensured in the event of a disaster or business disruption.
- 4.1.6 Security requirements must be identified, documented, and addressed in all phases of development or acquisition of information resources and satisfy all mandated federal compliance requirements.
- 4.2 Owner, Custodian, and User Responsibilities
- 4.2.1 Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented (see Appendix A).
- 4.3 Classification of Information
- 4.3.1 Each owner or custodian of information will determine classification based on the circumstances and the nature of the information.
- 4.3.2 The owner or custodian will determine the protective guidelines that apply for each level of information. They include the following:
- ? Access
 - ? Distribution within the DHHR
 - ? Distribution outside the DHHR
 - ? Electronic distribution
 - ? Disposal/Destruction (see 3.15, 3.16, and 3.17)
- 4.4 Resource Sharing
- 4.4.1 Information resources will be shared by all Bureaus/Offices within the DHHR in accordance with applicable state and federal confidentiality laws.
- 4.4.2 The DHHR will enable and promote interoperability within the DHHR through standardization, training, and the use of IT.
- 4.5 Managing Risks

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 4 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 4.5.1 Under the direction of the Information Security Officer (ISO), periodic risk analysis will be performed and documented.
- 4.5.2 Each Bureau/Office will maintain a cost effective business recovery plan that will provide for prompt and effective continuation of critical missions in the event of a disaster.
- 4.5.3 A regular review of the DHHR's information security program will be performed at least every two years by an individual(s) independent of the ISO and designated by the Chief Technology Officer (CTO).
- 4.6 Employee/Contractor Practices
- 4.6.1 Bureaus/Offices will use confidentiality agreements to document the acceptance of agency information security requirements.
- 4.7 Security Awareness and Training
- 4.7.1 The DHHR will provide ongoing information resources security awareness education for all users.
- 4.7.2 All employees accessing a mission critical application must receive appropriate training for using that application.
- 4.8 Enforcement Authority
- 4.8.1 The ISO is the person designated by the CTO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
- 4.8.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.
- 4.8.3 The OIG (Office of the Inspector General) is the authority who investigates reported instances of departmental employee misconduct.
- 4.9 Violations and Disciplinary Action(s)
- 4.9.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 5 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 4.9.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to the Office Director, Bureau Commissioner, or Community Services Manager (CSM) for appropriate action.
- 4.9.3 As determined by the Office Director or the Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.
- 4.9.4 Employees who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

- 5.1 Access – The ability to read, write, modify, or communicate data/information or otherwise use any system resource.
- 5.2 Chief Technology Officer (CTO) – The director of OMIS and the person responsible for all information resources within the DHHR.
- 5.3 Confidential Information – All information not in the public domain.
- 5.4 Control – A protective action, device, policy, procedure, technique or other measure that reduces exposure.
- 5.5 Custodian of an Information Resource – The unit or individual assigned to supply services associated with particular data. (see Appendix A)
- 5.6 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau /Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.7 Information Resources – A collection of manual and automated components, each managing a specific data set or information resource.
- 5.8 Interoperability – The ability of a system to use the parts or equipment of another system.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0512	REVISION: Original	PAGE 6 OF 6
SUBJECT: IT Information Security		EFFECTIVE DATE: 04/07/03	

- 5.9 Mission Critical Information – Information defined by the DHHR to be critical to the DHHR’s function(s).
- 5.10 Owner of an Information Resource – The individual(s) having primary responsibility for the creation and maintenance of the data content. (See Appendix A)
- 5.11 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
- 5.12 Security Breach – An event resulting in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether accidental or deliberate. (See Appendix A)
- 5.13 User of an Information Resource – The individual(s) who has been granted explicit authorization to access the data by the owners. (See Appendix A)

Attachment A

Roles and Responsibilities of Information Resource Owners, Custodians, and Users Within DHHR

Owners, Custodians, and Users of DHHR information resources must be approved by Bureau Commissioners, Office Directors, or a designee. Roles and responsibilities will be defined as follows:

- 1 **Owners** of information resources are responsible for the following:
 - 1.1 approving access and formally assigning custody of an asset;
 - 1.2 judging the asset's value;
 - 1.3 providing appropriate authority to implement security controls and procedures, and conveying them to users and custodians;
 - 1.4 protecting the DHHR's information resources, based on risk assessment, from unauthorized modification, deletion, or disclosure;
 - 1.5 maintaining information in the data file and ensuring that data is accurate and complete;
 - 1.6 classifying program information in concurrence with Bureau Commissioners; and
 - 1.7 advising the Information Security Officer (ISO) as to the designated owner in instances where information resources are used by more than one major program.
2. **Custodians** of information resources, including entities providing outsourced services to DHHR, are responsible for the following:
 - 2.1 implementing owner specified controls over the data;
 - 2.2 maintaining detailed knowledge of the data within their trust and reviewing usage information;
 - 2.3 providing physical and procedural safeguards for detecting, reporting, and investigating information security breaches;
 - 2.4 assisting owners in evaluating the cost-effectiveness of controls and monitoring; and

Attachment A

Roles and Responsibilities of Information Resource Owners, Custodians, and Users within DHHR

- 2.5 ensuring that DHHR employees comply with security procedures.
- 3 **Users** of information resources are responsible for the following:
 - 3.1 using data only for purposes specified by the owner;
 - 3.2 complying with security measures specified by the owner or custodian;
 - 3.3 protecting the data from unauthorized access and reporting information security information violations to the owner or the custodian; and
 - 3.4 concealing information in the data or the access controls over the data unless specifically authorized in writing by the owner.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 1 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE: 04/18/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy outlines the responsibilities and requirements of the Department of Health and Human Resources (DHHR) and its employees with regard to physical and environmental security for Information Technology (IT) resources.

2.0 SCOPE

This policy applies to all employees who use, service, and/or maintain the DHHR's information processing hardware, equipment, facilities, and/or resources.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 In instances where state and federal laws and regulations are more restrictive than DHHR IT policies, the more restrictive provisions will supersede.
- 3.2 The Health Insurance Portability and Accountability Act (HIPAA) of 1996
- 3.3 DHHR HIPAA Policy 0423 – Sanctions for Violating Privacy and Security Policies and Procedures
- 3.4 DHHR HIPAA Policy 0449 – General Guidelines to Safeguard Protected Health Information
- 3.5 DHHR IT Policy 0511, IT Network Security
- 3.6 DHHR IT Policy 0512, IT Information Security
- 3.7 DHHR IT Policy 0514, Disaster Recovery
- 3.8 DHHR IT Policy 0517, Media Disposal
- 3.9 DHHR Policy Memorandum 2104, Progressive Discipline
- 3.10 DHHR Policy Memorandum 2108, Employee Conduct
- 3.11 OMIS Operating Procedure (OP)-01, Computer Room Access
- 3.12 OMIS OP-17, Media Controls

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 2 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE: 04/18/05	

3.13 OMIS OP-18, Managing Information Security Incidents

4.0 RESPONSIBILITIES/REQUIREMENTS

4.1 DHHR Responsibility

- 4.1.1 Each Bureau/Office will develop a plan to maintain the physical security of IT Resources.
- 4.1.2 Each Bureau and/or Office will abide by rules governing physical access to stored information and information devices.
- 4.1.3 Each Bureau/Office should ensure that sufficient procedures relating to physical access to buildings are developed and maintained. Access procedures will vary according to the individual office location.
- 4.1.4 Each Bureau/Office must ensure that rooms and/or storage cabinets housing critical DHHR equipment, information assets, or access points must be restricted to only those who need access to fulfill their job responsibilities.
- 4.1.5 All DHHR employees are accountable for their actions relating to physical security, and will comply with policies and procedures protecting DHHR's computer assets and resources.
- 4.1.6 The DHHR will provide on-going awareness education, and train all employees on physical security requirements for IT resources.
- 4.1.7 The Information Security Officer (ISO) or a designee may conduct a physical security assessment of IT resources as needed.
- 4.1.8 The Office of Management Information Services (OMIS) will develop, review, and maintain policies and procedures relating to physical access to computing resources within the DHHR.

4.2 Access Control

- 4.2.1 Physical security controls for IT resources should be proportional to the risks of physical damage or unauthorized access.
- 4.2.2 All physical security provisions used for off-site storage will be equivalent to the standards of primary facilities and/or approved by the manager of the Network and Technical Support (NTS) unit.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 3 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

4.2.2.1 Periodic testing and review of physical security for IT resources plans will be conducted by OMIS .

4.2.3 Appropriate controls will be implemented to reduce the risk of sensitive information being transmitted to un-authorized persons. (Ex: confidentiality statements, outside e-mail encryption, etc.)

4.3 Environmental Security/Equipment

4.3.1 Each Bureau/Office should ensure that sufficient plans are developed and measures are put into place and maintained for protection against environmental factors (e g., dust, fire, power, or excessive heat and humidity).

4.3.1.1 Temperatures in server and switch rooms must stay between the range of 64 and 75 degrees. Humidity should remain between 30 to 55 percent.

4.3.2 Procedures will be established to ensure that computing resources are properly maintained.

4.3.3 Computing resources, including fax machines and printers, will be located in secure areas appropriate to the sensitivity of the output produced.

4.3.3.1 Employees are expected to be aware of equipment located within their immediate areas and to report missing equipment to supervisors.

4.3.4 All IT equipment should be carefully inspected prior to its disposal or release outside of DHHR to ensure that it contains no sensitive information, including any data remnants that might have been retained on the equipment after processing. (See OP-17, Media Controls)

4.4 Disaster Recovery (See IT-0514, Disaster Recovery)

4.4.1 Plans and controls will be in place to enable DHHR systems, on and off-site, to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

4.4.1.1 Each Bureau/Office will maintain a cost effective business recovery plan that will provide for prompt and effective continuation of critical missions in the event of a disaster.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 4 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

4.4.1.2 Each Bureau/Office will have procedures in place for reporting incidents, implementing the disaster recovery plan, and escalating the response to a disaster.

4.4.1.3 Each Bureau/Office is responsible for training, testing, and review of their disaster recovery plan(s).

4.5 Enforcement Authority

4.5.1 The ISO is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of the DHHR's information security program and IT policies.

4.5.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.

4.5.3 The Office of the Inspector General (OIG) is the authority who investigates reported instances of Departmental employee misconduct.

4.6 Violations and Disciplinary Action(s)

4.6.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.6.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to his/her Office Director or Bureau Commissioner for appropriate action.

4.6.3 As determined by the Office Director or Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.6.4 Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

5.1 Access – the ability to read, write, modify, or communicate data/information or otherwise use any system resource.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0513	REVISION: Original	PAGE 5 OF 5
SUBJECT: Physical Security for IT Resources		EFFECTIVE DATE 04/18/05	

- 5.2 Access Controls – rules for limiting access to safeguard systems and data at all times and under all conditions.
- 5.3 Chief Technology Officer (CTO) – the director of OMIS and the person responsible for all information resources within the DHHR.
- 5.4 Computing Resources – computer hardware, servers, PC's, workstations, terminals, printers, and other equipment physically located within the DHHR.
- 5.5 Disaster – Any event that makes an organization unable to provide critical business functions for a pre-determined period of time. This may include: any occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property resulting from a natural, technological, and/or national security incident, (ex: fire, vandalism, natural disaster, or system failure).
- 5.6 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractors' employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.7 Incident – An adverse event associated with an information system that: (1) fails to comply with security regulations or directives; (2) results in attempted or actual loss of data; (3) involves the waste, fraud, abuse, loss, or damage of property or information; and (4) reveals and/or exploits hardware or software vulnerabilities.
- 5.8 Office of Management Information Services (OMIS) - This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR
- 5.9 Physical Security – refers to the protection of building sites and equipment (and all other information and software contained within) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage.
- 5.10 Sensitive Information – Information/data that would be disadvantageous should it become known to others (ex: political/religious beliefs, health information, or criminal record).
- 5.11 Workstation – an electronic computing device (i.e., laptop or desktop computer), or any other device that performs similar functions, and the electronic media stored in its immediate environment.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 1 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE: 04/15/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

The purpose of this policy is to ensure that Department of Health and Human Resources (DHHR) data and electronic Protected Health Information (e-PHI) are protected from improper alteration or destruction in a manner proportionate to the associated risk when it is transmitted from one point to another.

2.0 SCOPE

This policy applies to all DHHR employees whose work or system support involves the transmission of e-PHI or other sensitive data.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 In instances where state and federal laws and regulations are more restrictive than DHHR IT policies, the more restrictive provisions will supersede.
- 3.2 The Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- 3.3 DHHR HIPAA Policy 0423 – Sanctions for Violating Privacy and Security Policies and Procedures
- 3.4 DHHR HIPAA Policy 0441 – Safeguards to Protect the Privacy of Protected Health Information
- 3.5 DHHR HIPAA Policy 0449 – General Guidelines to Safeguard Protected Health Information
- 3.6 DHHR IT Policy 0510 - E-Mail Guidelines and Requirements
- 3.7 Office of Management Information Services (OMIS) Operating Procedure (OP) -12 – E-Mail Guidelines
- 3.8 OMIS OP-18, Managing Information Security Incidents

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 3 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

- 4.4.2 OMIS will ensure that all systems containing e-PHI and other sensitive data are designed to maintain data integrity.
- 4.4.3 OMIS will conduct a risk analysis to ensure that e-PHI or sensitive data is reasonably protected from associated risks when transmitted from one point to another.
- 4.5 Data Owner Responsibilities
- 4.5.1 The data owner will review the results of a risk analysis to identify which data must be protected from improper alteration or destruction.
- 4.5.2 The data owner will coordinate with OMIS to ensure that all information containing e-PHI or sensitive data is protected from alteration during transmission.
- 4.5.3 The data owner(s) or designee(s) will keep a record of all e-PHI or sensitive data in each Bureau/Office.
- 4.6 Employee Responsibilities
- 4.6.1 Prior to transmission, employees must notify the data owner of any material containing e-PHI or sensitive data.
- 4.6.2 Employees are prohibited from using any DHHR system to store or transmit sensitive data or e-PHI that does not have adequate authorization mechanisms.
- 4.6.3 When transmitting e-PHI or sensitive data, regardless of the transmission system being used, employees must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the data requested.
- 4.7 Enforcement Authority
- 4.7.1 The ISO is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of the DHHR's information security program and IT policies.
- 4.7.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 4 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

4.7.3 The Office of the Inspector General (OIG) is the authority who investigates reported instances of Departmental employee misconduct.

4.8 Violations and Disciplinary Action(s)

4.8.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.8.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to his/her Office Director or Bureau Commissioner for appropriate action.

4.8.3 As determined by the Office Director or Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.8.4 Employees who willfully or knowingly violate or otherwise abuse the provisions to this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

5.0 DEFINITONS

- 5.1 Data owner – The person having primary responsibility for the creation and maintenance of the data content.
- 5.2 Electronic Protected Health Information (e-PHI) - Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.
- 5.3 Employee - Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purpose of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.4 Encryption – The process of enciphering or encoding data so that it is inaccessible to unauthorized users

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 5 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

- 5.5 Information Security Officer (ISO) – The person designated by the CTO to monitor and provide initial enforcement of DHHR’s information security program and IT policies.
- 5.6 Integrity – The ability for an entity to protect data from improper alteration or destruction and to assure e-PHI in its possession is kept consistent with its source.
- 5.7 LAN – A communications network made up of servers, workstations, a network operating system, and a communications link that serves users within a confined geographical area
- 5.8 Office of Management Information Services (OMIS) - This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
- 5.9 Virtual Private Network (VPN) - A way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 2 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

3.9 DHHR Policy Memorandum 2104 – Progressive Discipline

3.10 DHHR Policy Memorandum 2108 – Employee Conduct

4.0 RESPONSIBILITIES/REQUIREMENTS

4.1 Transmission Outside the DHHR Network

4.1.1 All transmission of sensitive data or e-PHI outside of the DHHR network must utilize an OMIS-approved Virtual Private Network (VPN).

4.1.1.1 Dedicated system-to-system connections do not require mandatory encryption controls.

4.2 Transmission Using E-Mail

4.2.1 All messages, attachments, files, and folders transmitted within the DHHR e-mail system are automatically encrypted.

4.2.2 E-mail transmitted outside the DHHR network is not encrypted, and should not be sent if the message or its attachment contains e-PHI.

4.3 Transmission Using Wireless LANs and Devices

4.3.1 The transmission of sensitive data or e-PHI over a wireless network within the DHHR is permitted only when the following conditions are met:

4.3.1.1 The wireless network is using the OMIS-approved authentication method to ensure that wireless devices connecting to the network are authorized; and

4.3.1.2 The wireless network is utilizing the OMIS standard encryption mechanism for all transmissions.

4.4 OMIS Responsibilities

4.4.1 OMIS will prescribe a comprehensive internal security control program to protect e-PHI and other sensitive data from improper alteration or destruction, and keep it consistent with its source

Office of Management Information Services (OMIS) Operating Procedure

OP-14 – User Security

Effective: 04/27/04

Revised: 05/18/05

1.0 PURPOSE

This Operating Procedure (OP) defines the responsibilities of all Department of Health and Human Resources (DHHR) employees with regard to user/workstation security.

2.0 SCOPE

This OP applies to all employees accessing DHHR supported applications and computer systems. It also applies to personnel from other departments, agencies, contractors, and vendors using DHHR's data communications system(s) or networks.

3.0 PROCEDURE

3.1 Employee Security

- 3.1.1 All employees are required to be aware of and comply with applicable IT security policies and procedures. These can be accessed at:
<http://www.wvdhhr.org/mis/IT/index.htm>.
- 3.1.2 Employees will always lock or log-off PC's when leaving their workstations (lunch, breaks, and/or meetings), in the event of an emergency (time permitting), or when leaving for the day.
 - 3.1.2.1 Instructions on locking or logging off computers can be found at:
<http://intranet.wvdhhr.org/itops/index.htm>.
- 3.1.3 Employees should save all open work before locking or logging off computers to prevent accidental loss of data.
 - 3.1.3.1 OMIS reserves the right to unlock any DHHR computer at any time. In this event, the current user will be logged off, and any unsaved data will be lost.
- 3.1.4 Employees will backup important information according to IT policy guidelines (see [IT-0511](#), IT Network Security).
 - 3.1.4.1 All important information must be stored on network drives.

Office of Management Information Services (OMIS)

Operating Procedure

OP-14 – User Security

Effective: 04/27/04

Revised: 05/18/05

3.1.4.2 Employees must request approval from OMIS in order to gain access to another person's Y: drive.

3.1.4.2.1 Requests must be sent by memo or e-mail to the OMIS Help Desk.

3.1.5 Employees will always restrict the use of important/confidential information to a need-to-know basis.

3.2 Passwords

3.2.1 Employees will always use strong passwords, which must be a combination of as many different groups of characters as possible (ex: upper and lower case letters, numbers, symbols, and punctuation). For rules on e-mail passwords, see OP-12.

3.3 Userids

3.3.1 Each employee will be assigned a unique identifier (userid). The actions of an employee should be traceable to that employee.

3.2.1.1 All network and mainframe userid's will be assigned by the Office of Management Information Services' (OMIS)

3.2.1.2 Other system/application userid's will be assigned by the data owner.

3.3.2 A single userid will not be permitted to sign on to a system or application from more than one physical workstation at a time, except for authorized computer support personnel for authorized purposes.

4.0 ABUSE/VIOLATIONS

Violations of this OP will subject an individual to disciplinary action in accordance with DHHR Policy Memorandum 2104, Progressive Discipline. Depending on the circumstances surrounding the incident, OP violations could result in prosecution under state and federal statutes.

5.0 DEFINITIONS

Office of Management Information Services (OMIS) Operating Procedure

OP-14 – User Security

Effective: 04/27/04

Revised: 05/18/05

- 5.1 Backup – To copy files from one storage area, especially a hard disk, to another to prevent their loss in case of a disk failure.
- 5.2 Confidential Information – All information not in the public domain.
- 5.3 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this OP. For the purpose of this OP, this also refers to anyone using a computer connected to the DHHR network.
- 5.4 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.

Office of Management Information Services (OMIS) Operating Procedure

OP-21 - Security Management Process

Effective: 04/12/05

1.0 PURPOSE

This Operating Procedure (OP) identifies the security management process within the Department of Health and Human Resources (DHHR), which may include risk analysis, as well as documentation and review of system vulnerabilities and information system activity.

2.0 SCOPE

This OP applies to all DHHR employees.

3.0 PROCEDURE

3.1 Risk Analysis

3.1.1 The Office of Management Information Services (OMIS) will oversee an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of DHHR data. This analysis will accomplish the following:

3.1.1.1 Identify potential threats and probabilities;

3.1.1.2 Determine what the relevant losses would be if security measures were not in place; and

3.1.1.3 Determine whether appropriate security measures have or need to be taken to reduce vulnerabilities.

3.1.2 The risk analysis must be documented, retained for six years, and should be periodically reassessed and updated annually (at a minimum).

3.2 Risk Management Process

3.2.1 OMIS will implement, maintain, and document all security measures to reduce risks and vulnerabilities to a reasonable and appropriate level. This process includes, but is not limited to the following:

3.2.1.1 Threat event: What could happen?

3.2.1.2 Threat impact: If it happened, how bad could it be?

Office of Management Information Services (OMIS) Operating Procedure

OP-21 - Security Management Process

Effective: 04/12/05

- 3.2.1.3 Threat frequency: How often could it happen?
- 3.2.1.4 Threat probability: How likely is the threat event?
- 3.2.2 To complete the risk management process, the following three questions should be answered:
 - 3.2.2.1 How can risk be mitigated?
 - 3.2.2.2 What is the annual cost?
 - 3.2.2.3 What is the cost/benefit ratio?
- 3.3. Information System Activity Review
 - 3.3.1 OMIS will implement internal audits to regularly review records of system activity.
 - 3.3.1.1 Audits may utilize logs, activity reports, or other mechanisms to document and manage system activity.
 - 3.3.1.2 Audits must be conducted at a frequency proportionate with the associated risk of the information system.
 - 3.3.1.3 System activity logs must include, but are not limited to the following information:
 - 3.3.1.3.1 Failed and successful log-in attempts; and
 - 3.3.1.3.2 Permission/access authorization changes
 - 3.3.2 An audit plan must be created and approved by OMIS for each system
 - 3.3.3 Security incidents such as activity exceptions and unauthorized access attempts must be detected and logged. Breaches must be reported immediately according to the requirements found in OP-18, *Managing Information Security Incidents*.
 - 3.3.3.1 Data owners will develop procedures for system and/or application activity review for their area(s) of responsibility.

Office of Management Information Services (OMIS) Operating Procedure

OP-21 - Security Management Process

Effective: 04/12/05

4.0 ABUSE/VIOLATIONS

Violation of this OP will subject an individual to disciplinary action in accordance with DHHR Policy Memorandum 2104 - *Progressive Discipline*, and with DHHR HIPAA Policy 0423 - *Sanctions for Violating Privacy and Security Policy and Procedures*. Depending on the circumstances surrounding the incident, OP violations could result in prosecution under state and federal statutes.

5.0 DEFINITIONS

- 5.1 Chief Technology Officer (CTO) – The director of MIS and the person responsible for all information resources within the DHHR.
- 5.2 Data Center Desktop Support (DCDS) – The OMIS organization that is responsible for the DHHR Data Center and the Kanawha County offices.
- 5.3 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this OP. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.4 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.
- 5.5 Risk Analysis – A process where relevant assets and threats are identified, and cost-effective security/control measures are identified or engineered to effectively balance the costs of various security/risk mitigation/control measures against the losses that would be expected if these measures were not in place.
- 5.6 Risk Management – The process of analyzing exposure to risk and determining how to best handle such exposure.

Office of Management Information Services (OMIS) Operating Procedure

OP-22 – Information Security (InfoSec) Awareness Training

Effective: 04/15/05

1.0 PURPOSE

This Operating Procedure (OP) provides an overview of the responsibilities of all Department of Health and Human Resources (DHHR) employees with regard to Information Security (InfoSec) awareness training within the DHHR. It also outlines responsibilities of the DHHR Information Security Officer (ISO).

2.0 SCOPE

This OP applies to all DHHR employees.

3.0 PROCEDURE

3.1 Each Bureau/Office will ensure that all employees have been trained in and understand all DHHR InfoSec policies and/or OPs. This may include training pertaining to the following:

- 3.1.1 InfoSec awareness;
- 3.1.2 Physical security;
- 3.1.3 Confidentiality;
- 3.1.4 Virus protection;
- 3.1.5 Password management;
- 3.1.6 Monitored log-in attempts; and
- 3.1.7 Employee sanctions for privacy and InfoSec violations.

3.2 Each Bureau/Office may train employees using the following methods:

- 3.2.1 Online web training;
- 3.2.2 Intranet and/or E-mail reminders;
- 3.2.3 Group training sessions;
- 3.2.4 Verbal updates; and

Office of Management Information Services (OMIS) Operating Procedure

OP-22 – Information Security (InfoSec) Awareness Training

Effective: 04/15/05

- 3.2.5 Posters/bulletin boards/flyers
- 3.3 The ISO or designee will provide and oversee InfoSec awareness training for all employees.
 - 3.3.1 Each Bureau/Office will designate a training attendance monitor who will be responsible for documenting employee InfoSec training. This individual's contact information must be provided to the ISO or designee.
 - 3.3.2 Each new employee will be required to complete InfoSec awareness training via the Intranet. Employees without Intranet access will receive an alternate training method.
 - 3.3.2.1 Upon completion of the training, employees must print and sign the training completion certificate, then submit it to the section manager/supervisor within three working days.
 - 3.3.2.2 The training attendance monitor must submit an employee training completion roster to the ISO or designee at least quarterly.
 - 3.3.3 Established employees will be required to complete a review of InfoSec awareness training annually. This review will be provided via the Intranet or an alternate method.
 - 3.3.3.1 Notification and due date of the annual training review will be distributed to employees via E-mail or alternate method.
 - 3.3.3.2 Upon completion of the training, employees must print and sign the training completion certificate, then submit it to the section manager/supervisor within 20 working days after training materials are made available.
 - 3.3.3.3 The training attendance monitor must submit an employee training completion roster to the ISO or designee at least quarterly.
- 3.3.4 All employees will be notified of policy and/or OP changes deemed critical by the Chief Technology Officer (CTO).

Office of Management Information Services (OMIS) Operating Procedure

OP-22 – Information Security (InfoSec) Awareness Training

Effective: 04/15/05

- 3.3.4.1 Details of policy and/or OP revisions will be made available to employees via the Intranet, E-mail, or alternate method.
- 3.3.4.2 Employees must sign a training completion roster, provided by the training attendance monitor, acknowledging receipt of policy and/or OP revision(s).
- 3.3.4.3 The training attendance monitor must submit the roster to the ISO or designee, by a date as requested by the ISO.
- 3.4 The ISO or designee will provide the DHHR HIPAA Privacy Officer with a copy of formal training materials and training attendance documentation pertaining to electronic Protected Health Information (e-PHI) policy and OP training.
 - 3.4.1 The ISO or designee will consult with the DHHR HIPAA Privacy Officer concerning e-PHI training materials in advance of training.
 - 3.4.2 The ISO or designee must offer the DHHR HIPAA Privacy Officer a copy of any revisions to formal training materials pertaining to e-PHI or sensitive data.
 - 3.4.2.1 The HIPAA Privacy Officer will retain copies of PHI training material in accordance with HIPAA Policy 0422, *Training Program: Uses, Disclosures, and Safeguarding Protected Health Information*.
- 3.5 The ISO or designee will periodically provide reminders relating to InfoSec issues and safeguards to the E-mail administrator for distribution to employees. Employees without E-mail access will receive reminders from local supervisors via an alternate method.

4.0 ABUSE VIOLATIONS

Violation of this OP will subject an individual to disciplinary action in accordance with DHHR Policy Memorandum 2104 - *Progressive Discipline*, and with DHHR HIPAA Policy 0423 - *Sanctions for Violating Privacy and Security Policy and Procedures*. Depending on the circumstances surrounding the incident, OP violations could result in prosecution under state and federal statutes.

Office of Management Information Services (OMIS) Operating Procedure

OP-22 – Information Security (InfoSec) Awareness Training

Effective: 04/15/05

5.0 DEFINITIONS

- 5.1 Chief Technology Officer (CTO) – The director of OMIS. The CTO is responsible for all information resources within the DHHR.
- 5.2 DHHR HIPAA Privacy Officer – Individual designated by the DHHR, who is responsible for the development and implementation of privacy policies and procedures for the purposes of HIPAA privacy regulations.
- 5.3 Electronic Protected Health Information (e-PHI) – Health information transmitted by or maintained in electronic media used to identify an individual, which is created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.
- 5.4 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this OP. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.
- 5.5 Information Security Officer (ISO) – Individual designated by the CTO to monitor and provide initial enforcement of the DHHR's information security program and IT policies.
- 5.6 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.