

12-0287

FILED
2012 JAN 23 PM 2:34
CATHY GATSON, CLERK
KANAWHA COUNTY CIRCUIT COURT

IN THE CIRCUIT COURT OF KANAWHA COUNTY, WEST VIRGINIA

WEST VIRGINIA DEPARTMENT OF TRANSPORTATION/
DIVISION OF HIGHWAYS,

Petitioner,

v.

Civil Action No. 11-AA-132
Judge Tod J. Kaufman

KENNETH R. LITTEN,

Respondent.

FINAL ORDER

Before the Court is Petitioner's Petition for Appeal filed on December 9, 2011. Petitioner in this case, Respondent below, the Division of Highways (hereinafter "DOH" or "Petitioner") is appealing the West Virginia Public Employee's Grievance Board's ("Board") decision that held the Petitioner failed to meet its burden by showing that the Respondent in this case, the Petitioner below, Mr. Kenneth Litten (hereinafter "Respondent"), violated the West Virginia Office of Technology's ("OOT") policy when he allegedly accessed pornographic websites on the state's computer by a preponderance of the evidence. The Board granted the Respondents's grievance, ordered him reinstated to his job as a Mechanic at the District 5 Burlington Headquarters, and awarded back pay.

Factual and Procedural Background

Prior to his dismissal, the Respondent had been employed by the Division of Highways (hereinafter "DOH"), in the Shop at the District 5 Headquarters in Burlington, West Virginia, for eleven years, and was a Mechanic 3.

The Respondent was notified on November 16, 2010 that a recommendation had been



made that he be dismissed from his employment. The Respondent denied the allegations against him. By letter dated November 29, 2010, Jeff Black, Director of Human Resources for DOH, notified the Respondent that his employment was terminated effective December 15, 2010, for “violation fo the West Virginia Office of Technology’s policies on Information Security and Network Violation Management, and the Department of Transportation’s policy regarding Proper use of Information Technology. More specifically:

On August 27, 2010, during the hours of 10:00 a.m. and 2:00 p.m., you visited and attempted to visit numerous known pornographic websites. You were denied access to over 400 requested sites or files that are categorized as known pornography or offensive search engine keywords. The Office of Technology was able to trace these activities to the IP address for your computer, 10.69.205.18,¹ and your unique user identification, A073191. Due to the serious nature of this offense, coupled with your prior discipline for misuse of state resources, your dismissal is warranted.”

The West Virginia OOT monitors computer usage by state employees in an effort to protect the statewide network from the introduction of viruses and malware which could harm the network. OOT has identified websites which are known to put the network at risk for viruses and malware and blocks access to these websites. These websites include those considered by OOT to be pornographic. When an employee attempts to access these types of websites, OOT is alerted to the possible network violation, and OOT personnel then review the activity for a period

¹ This was not the Respondent’s computer, but a computer used by the Respondent and other mechanics at the Respondent’s worksite. The Respondent did not have a computer assigned to him.

of time to determine whether a violation has occurred. Employees can employ various techniques to defeat the blocked access to websites.

The Department of Transportation also has a policy in place which prohibits employees of DOH from accessing “potentially threatening, offensive, or harassing information, “ including “material that could be construed as . . . obscene, pornographic, profane, sexually oriented or sexually explicit . . . or otherwise inappropriate or illegal.”

Prior to August 27, 2010, the Respondent had taken most if not all of the online training course provided by OOT on computer information security. This training included information on the importance of safeguarding the network by not accessing pornographic and other non-secure, non-work-related websites, and the importance of safeguarding each individual’s password. The Respondent had also been made aware, through other training, of the importance of safeguarding his password.

OOT’s Information Security Policy states at Section 4.17 that “[e]ach employee must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.” The stated purpose of the Information Security Policy is to establish “objectives and responsibilities for all West Virginia state government agencies, employees, vendors, and business associates, specifically the Executive, regarding information security and the protection of information resources. This Policy further provides at Section 5.2.3 that “[e]mployees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following: Logging off computer”

OOT’s Information Security Policy states at Section 4.14 that “controls must be

established and maintained to protect the confidentiality of passwords,” and “passwords are confidential and must not be shared under any circumstances.”

The Respondent was not assigned his own computer, but he had been assigned his own user identification number which he used to sign onto the computer located in the break room. The Respondent’s co-workers in the District 5 Shop at Burlington also used this computer. The Respondent had his own password.

When he was first assigned a user identification number, the Respondent wrote his user identification number, except the first letter, on the front of the community sheet of paper which outlined the procedure for logging onto the computer, and he wrote his password on the back of this paper. This paper was on the bulletin board beside the computer in the break room shared by the employees. The Respondent’s first password was Sissy9, and this was written in blue ink on the back of the login document, with a capital s (S) written in overtop of a lower case s (s).

Every 30 days, the Respondent was required to change his password, and he did so by changing the number in his password to the next number. Below the 9, written in blue ink, was the number 10, reflecting that he had changed his password to Sissy10, and below that, in blue ink, was the number 11, for Sissy11. Below, 11, written in black ink, was the number 12, and then below that, in black ink, was the number 13. There is room on the document for only one or two more numbers below the space where the 13 is written. No additional numbers were recorded on the document. By the time the Respondent was dismissed from his employment, his password was Sissy25.

The Respondent did not properly safeguard his password.

There are nine Mechanics, one Welder, a Shop Foreman, an Office Assistant, an

Equipment Supervisor, and an Assistant to the Equipment Supervisor assigned to the District 5 Shop at Burlington.

On August 30, 2010, personnel in OOT became aware , during a routine review of activity, that on August 27, 2010, someone had attempted to access pornographic websites utilizing the Respondent's user identification number, between the hours of 10:00 a.m. and 2:00 p.m. The "identified computer was denied access to over 400 requests to sites or files that were categorized as known pornography or offensive search engine keywords,' as defined by OOT. The pictures on at least some of these websites were, at the very least, sexually oriented and sexually explicit.

When OOT personnel were alerted to the fact that someone using the Respondent's identification number had attempted to access websites classified by OOT as pornographic, OOT personnel reviewed the activity on the computer for a 24-hour period surrounding the time period on August 27, 2010. In the course of this review, OOT personnel general a "Network Violation Report, " which summarized the inappropriate search on August 27, 2010, the times of the searches, search terms, and pictures from websites, which had been accessed using the Respondent's identification number. The Network Violation Report was provided to DOH.

This was the first time the OOT had generated a Network Violation Report for the Respondent's user identification number.

No one observed the Respondent accessing or attempting to access pornographic or sexually explicit websites on August 27, 2010.

When the Mechanics work on a piece of equipment, they record those hours on a work order. The beginning and ending time recorded may not be exact, as they record their time to the

nearest half hour.

On August 27, 2010, Delbert J. "D.J." Streets, a Mechanic employed by DOH at the Burlington Headquarters, began working on a crane around 7:30 a.m. Before he could begin repairs, he had to move the crane to the work area. The Respondent assisted Mr. Streets with the repairs, joining him around 7:30 a.m., or very soon thereafter. The work order completed by the Respondent, and accepted by his supervisor, shows that the Respondent worked on the crane from 6:30 a.m. until 9:00 a.m. Prior to Mr. Streets moving the crane, the Respondent had looked at it to determine what work needed to be completed on it in order to correct the problem. Mr. Streets did not see the Respondent when he moved the crane to the work area around 7:30 a.m.

Someone logged onto the computer in the break room using the Respondent's identification number and password at 7:16 a.m. While the Respondent's identification number was logged onto the computer, websites classified by OOT as pornographic were accessed, or access was attempted and denied.

When the Respondent finished working on the crane on August 27, 2010, he began working on a box truck, helping Shane Dolly, a Mechanic employed by DOH at the Burlington Headquarters. The work order completed by the Respondent shows that he worked on the box truck from 9:00 a.m. to 11:30 a.m. Mr. Dolly recorded his time working on the box truck as 8:00 a.m. to 11:00 a.m. After the Respondent and Mr. Dolly completed the work on the box truck, the Respondent put away the ladders and other tools and equipment they had been using in repairing the box truck.

Someone logged onto the computer in the break room using the Respondent's identification number and password at 9:53 a.m. While the Respondent's identification number

was logged onto the computer, websites classified by OOT as pornographic were accessed, or access was attempted and denied.

The Respondent took his lunch break between 11:30 a.m. and 12:00 p.m. on August 27, 2010. There was no improper computer usage during this time period under the Respondent's user identification number and password.

Michael Eversole, a Mechanic at the DOH Burlington Headquarters, worked on a pickup truck on August 27, 2010, from 11:00 a.m. until 3:30 p.m. The Respondent assisted him with the repairs on this truck. The work order shows the Respondent worked on this truck from 12:00 p.m. to 3:30 p.m.

Someone logged onto the computer in the break room using the Respondent's identification number and password at 12:30 p.m. While the Respondent's identification number was logged in, websites classified by OOT as pornographic were accessed, or access was attempted and denied.

The Respondent worked 47.5 hours during the week of August 27, 2010, and 7.5 of the 8 hours worked on August 27, 2010, were overtime.

The Respondent was suspended for ten days without pay in 2009 for misuse of state equipment.

The Respondent was viewed as a good employee who was always willing to help his co-workers with diagnosing mechanical problems and making repairs. His experience was an asset in diagnosing mechanical problems. The Respondent's last performance evaluation was completed in September of 2010, covering the period from January 1 through December 31, 2009. He received a rating of meets expectations. He was rated as exceeds expectations in eight

of the twenty-three categories and was not rated as needing improvement in any category.

The Petitioner has consistently imposed a fifteen-day suspension on employees who are not supervisors for a first offense of accessing or attempting to access pornographic websites on a state computer, resulting in the generation of a Network Violation Report, a twenty-day suspension for a first offense if the employee is a supervisor, and dismissal for a second offense of this same type.

The petitioner did not consider the Respondent's tenure or work history in determining whether the Respondent should be dismissed.

In November of 2010, DOH employees were required to use a computer to enter information regarding their job duties and responsibilities on a job comparison questionnaire to be submitted to the Division of Personnel. Many of the employees at the Burlington Headquarters did not feel competent to perform this task or did not want to do it, so the secretary in the office, Debra Aman, offered to do this for them. However, in order to complete this task, Ms. Aman had to enter the data under the user identification number for each employee, and the employees provided their passwords to her. Many of the employees gave Ms. Aman their passwords. D.J. Streets saw that Ms. Aman was having difficulty getting all the data entered and had become stressed, so he told her he would enter the data for his job. Then he asked if she would like for him to enter the data for other employees, Ms. Aman gave him the user identification number and password for another employee, and he entered the data.

The OOT takes password security seriously and considers the sharing of passwords and the failure to protect a password to be a more serious violation than accessing pornographic websites because these acts put the network at higher risk than accessing pornographic websites.

If an unauthorized person is able to access the network, he can transfer files to an iPod or thumb drive, and there will be no record left for the audit trail. Also, a person could introduce viruses, Trojans, and other malicious software, whereas someone accessing a pornographic website leaves a trail that can be followed by OOT personnel to repair any damage. OOT views the individual's password as so sensitive that it should never be shared with anyone, including OOT personnel.

None of the employees who gave Ms. Aman their passwords was disciplined for this violation of OOT policy.

During the Summer of 2010, DOH hired five summer workers in District 5. DOH did not obtain identification numbers for these temporary employees so that they could log onto a computer with their own number and password and enter their time. Leslie Stagers, the District 5 Human Resources contact person, made the decision to allow these five temporary employees to use the identification numbers assigned to five full-time employees who did not use the computer, using a password chosen by the temporary employees. DOH considered this to be a violation of OOT policy, but Ms. Stagers was not disciplined for this misuse of personal employee identification numbers.

Standard of Review

This Court's review is governed by the West Virginia Administrative Procedures Act, W.Va. Code § 29A-5-1 *et seq.* West Virginia Code § 29A-5-4(g) states:

The court may affirm the order or decision of the agency or remand the case for further proceedings. It shall reverse, vacate or modify the order or decision of the agency if the substantial rights of the petitioner or petitioners have been prejudiced because the administrative findings, inferences, conclusions, decision or order are:

- (1) In violation of constitutional or statutory provisions; or
- (2) In excess of the statutory authority or jurisdiction of the agency; or
- (3) Made upon unlawful procedures; or
- (4) Affected by other error of law; or
- (5) Clearly wrong in view of the reliable, probative and substantial evidence on the whole record; or
- (6) Arbitrary or capricious or characterized by abuse of discretion or clearly unwarranted exercise of discretion.

The Court must give deference to the administrative agency's factual findings and reviews those findings under a clearly wrong standard. Further, the Court applies a *de novo* standard of review to the agency's conclusions of law. *Muscatell v. Cline*, 474 S.E.2d 518, 525 (W.Va. 1996).

Discussion

In its Petition, the Petitioner states that the Administrative Law Judge ("ALJ") committed substantial legal error by altering the standard and burden of proof and requiring direct evidence, by excluding relevant evidence regarding the identity of the user who committed the violations; and by construing the technological reports in a manner contrary to the only evidence of record. After careful review of the briefs, the record, and the relevant law, the Court has concluded that the Petitioner has failed to establish a basis for reversing the ALJ's final order.

In reviewing whether the record supports the ALJ's decision, it is important to keep in mind that the reason for terminating the Respondent was that he was allegedly accessing or attempting to access pornographic materials on a specific date, August 27, 2010, in the break room of District 5 Burlington Headquarters. In disciplinary matters, the burden of proof rests with the employer, and the employer must show by a preponderance of the evidence that the discipline against the employee was proper. See *Ramey v. W.Va. Dep't of Health*, Docket No. H-

88-005 (Dec. 6, 1988). “The preponderance standard generally requires proof that a reasonable person would accept as sufficient that a contested fact is more likely true than not.” *Leichliter v. W. Va. Dep’t of Health and Human Res.*, Docket No. 92-HHR-486 (May 17, 1993). Where the evidence equally supports both sides, the employer has not met its burden. *Id.* Therefore, the Respondent had the burden to prove and failed to prove by a preponderance of the evidence that the Respondent did access or attempt to access pornographic materials on the computer in the break room, and the resulting termination was inappropriate.

Additionally, the Court in *Clarke* stated, “Where an act of misconduct is asserted in a notice of dismissal, it should be identified by date, specific or approximate, unless the characteristics are so singular that there is no reasonable doubt when it occurred. If an act of misconduct involves persons or property, these must be identified to the extent that the accused employee will have no reasonable doubt as to their identity.” Syl. Pt. 2, *Clarke v. W. Va. Bd. Of Regents*, 279 S.E.2d 169 (W. Va. 1981), citing Syl. Pts. 4 and 5 of *Snyder v. Civil Serv. Comm’n*, 238 S.E.2d 842 (W. Va. 1977). The charges against the Respondent, as stated in the dismissal letter, were that on August 27, 2010, during the hours of 10:00 a.m. and 2:00 p.m., he visited and attempted to visit numerous known pornographic websites.

The record in this case does not show that the ALJ excluded relevant evidence regarding the identity of the user who committed the violations. Rather the record reflects that the ALJ heard and carefully considered all of the evidence before it, including the testimony of DOH witnesses that had previously seen the Respondent on pornographic websites and hearsay, and concluded that the Petitioner failed to demonstrate that the Respondent was the user who was trying to access pornographic websites. The ALJ explained in detail what testimony and evidence

was relevant and furthermore, how it supported the conclusions made. The ALJ relied heavily on the evidence that although the DOH had numerous witnesses that had previously seen the Respondent on pornographic websites on the computer in the break room, not a single witness could place the Respondent in the chair on August 27, 2010 between the hours of 10:00 a.m. and 2:00 p.m., which is the only date and time period listed in the Respondent's dismissal letter. Furthermore, the ALJ had discretion to comport with date and time frame listed in the dismissal letter. Accordingly, this Court finds that the ALJ did not err in relying on testimony and evidence that complied with the date and time frame the Petitioner listed in its dismissal letter to the Respondent.

Regarding the ALJ's discussion of logoff times, this Court finds that the ALJ was mistaken when she assumed the Respondent would need to be missing from work for approximately two hours on August 27, 2010 in order to be the user accessing or attempting to access pornographic websites. Mr. James Weathersby of the OOT testified that there was in fact no way to tell from the report entered into evidence when someone logged off. In fact, he claimed that a login attempt code (520) and a logoff attempt code (540) were different, but the OOT does not include the logoff times in its report because relying on such code is not always accurate. Additionally, he testified that there are "a lot of different things that it logs off at various times, and we don't have a mechanism to show when the individual *actually* logged off the PC." Transcript, 54 (July 28, 2011)(emphasis added).

Therefore, this Court finds that the ALJ was mistaken when she included and relied on logoff times in her discussion; however, even absent this mistake, the Petitioner cannot place the Respondent in the chair as the one accessing or attempting to access pornographic websites on

August 27, 2010 between the hours of 10:00 a.m. to 2:00 p.m. Thus, this Court holds that the ALJ's finding was not clearly erroneous.

Ruling

After carefully reviewing the decision below, the Petitioner's brief, the Respondent's brief, the record, and the relevant law, the Court hereby AFFIRMS the decision of the Board below because the evidence in the record supports the findings of fact and conclusions of law. This case is DISMISSED and STRICKEN from the docket of the Court.

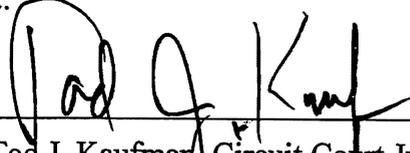
The clerk of the court shall distribute copies of this Order to all parties of record:

Krista D. Black, Esquire
WV Department of Transportation/
Division of Highways
Room 517, Building Five
1900 Kanawha Blvd., East
Charleston, WV 25305

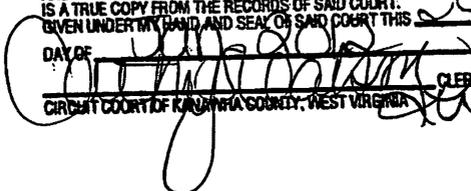
Katherine L. Dooley, Esquire
1600 Third Avenue
P.O. Box 11270
Charleston, WV 25339

WV Public Employees Grievance Bd
1596 Kanawha Blvd., East
Charleston, WV 25311

Enter this Order the 23 day of January, 2012.



Tod J. Kaufman, Circuit Court Judge for
Kanawha County

STATE OF WEST VIRGINIA
COUNTY OF KANAWHA, SS
I, CATHY S. GATSON, CLERK OF CIRCUIT COURT OF SAID COUNTY
AND IN SAID STATE, DO HEREBY CERTIFY THAT THE FOREGOING
IS A TRUE COPY FROM THE RECORDS OF SAID COURT.
GIVEN UNDER MY HAND AND SEAL OF SAID COURT THIS 24
DAY OF JANUARY 2012.


CATHY S. GATSON, CLERK
CIRCUIT COURT OF KANAWHA COUNTY, WEST VIRGINIA