

Issue: Group II Written Notice with 10-day suspension (internet abuse); Hearing Date: 01/21/03; Decision Issued: 02/07/03; Agency: VDOT; AHO: Carl Wilson Schmidt, Esq.; Case No. 5614



COMMONWEALTH of VIRGINIA
Department of Employment Dispute Resolution

DIVISION OF HEARINGS

DECISION OF HEARING OFFICER

In re:

Case Number: 5614

Hearing Date: January 21, 2003
Decision Issued: February 7, 2003

PROCEDURAL HISTORY

On October 2, 2002, Grievant was issued a Group II Written Notice of disciplinary action with ten workday suspension for failing to follow the Agency's policy regarding internet use. On November 1, 2002, Grievant timely filed a grievance to challenge the disciplinary action. The outcome of the Third Resolution Step was not satisfactory to the Grievant and he requested a hearing. On December 17, 2002, the Department of Employment Dispute Resolution assigned this appeal to the Hearing Officer. On January 21, 2003, a hearing was held at the Agency's regional office.

APPEARANCES

Grievant
Grievant's Representative
Agency Party Designee
Agency Advocate
Internal Auditor
Audit Director
Facility Director
Information Technology Specialist
Traffic Controller

Traffic Control Supervisor

ISSUE

Whether Grievant should receive a Group II Written Notice of disciplinary action with suspension for failure to follow established written policy.

BURDEN OF PROOF

The burden of proof is on the Agency to show by a preponderance of the evidence that its disciplinary action against the Grievant was warranted and appropriate under the circumstances. Grievance Procedure Manual ("GPM") § 5.8. A preponderance of the evidence is evidence which shows that what is sought to be proved is more probable than not. GPM § 9.

FINDINGS OF FACT

After reviewing the evidence presented and observing the demeanor of each witness, the Hearing Officer makes the following findings of fact:

The Virginia Department of Transportation employs Grievant as a Traffic Controller. He and one or more employees sit at a three panel workstation. Grievant's supervisor sits directly behind Grievant and monitors Grievant's actions and the actions of other staff working in the room. Grievant must frequently respond to radio calls and other activities while working. No evidence of prior active disciplinary action against Grievant was introduced.

Agency employees can access the internet using personal computers connected to the Agency's computer network. The Agency maintains a firewall securing the network. A firewall is software designed to protect the network from unauthorized access by persons outside of the network and to monitor usage of those within the computer network. When an employee uses an Agency computer to access the internet, the firewall software records the name of the person logged onto the personal computer and the website accessed by that computer. This is accomplished by assigning an internet protocol (IP) address to the personal computer and monitoring the uniform resource locator (URL) accessed by that computer.

Staff at the Office of the Attorney General received a complaint that a VDOT employee was accessing pornographic sites through the internet. VDOT investigated the allegation and determined it to be founded. The Agency concluded that if one employee was using the internet inappropriately, others may also be using the internet inappropriately.

Determining whether employees have inappropriately used their computers is time consuming and expensive.¹ Rather than reviewing the internet usage for several thousand employees, the Agency decided to target the employees with the highest usage of the internet and then determine if their usage was inappropriate. Agency auditors determined that, “the generation of 10,000 or more log records in one day from a single IP address was a good indicator that a ‘substantial’ abuse of the Internet facility could be taking place from the related PC.”² Auditors reviewed the firewall log for the week of April 8th to 14th, 2002 (“review week”). They identified 93 unique IP addresses meeting or exceeding the 10,000 records on one or more than one day of the week reviewed.

For each of the 93 unique IP addresses, the auditors selected one day during the review week with the highest number of records generated and further examined activity during that day. The auditors considered as non-work activity, those websites accesses that fall into the categories of:

1. General non-work related activities, which includes sports, shopping (retailers and auction), movie and movie news, music, dating, vacations and travel, etc.
2. Sexually Explicit Material
3. Gambling
4. Terrorism
5. Drug abuse.

Auditors reviewed the activity for each IP address and determined how much time was devoted to non-work activity³. Once the auditors concluded they had identified at least two hours of non-work activity, they discontinued further review of the websites accessed by the computer. In essence, the auditors concluded that at least two hours of non-work related activity was sufficient to refer the matter to Agency managers for disciplinary action.

¹ DHRM Policy 1.75, Use of Internet and Electronic Communication Systems, informs State employees that they should not have any expectation of privacy when using Agency equipment to access the internet and that agencies have the right to monitor employee usage.

² Agency Exhibit 2. The auditors also noted that although “a much lower number of log records can also represent a substantial Internet use, ... we do not have resources to investigate these at the present time.”

³ Non-work activity can be difficult to measure. For example, if an employee visits a non-business related website and then turns away from the computer to perform work duties while leaving the website on the computer, the firewall would register the employee being engaged in non-work activity even though the employee had begun performing his or her job. To avoid this problem, the auditors assumed that if the firewall showed no activity for more than a minute, then the employee had turned away from the computer to perform work activities. No time was added towards the two hour benchmark. An example of this situation would be an employee who frequently clicks on websites for four minutes and then stops accessing any websites for more than one minute. Even though the last website accessed by the employee was not business related, the auditors would not count the time beyond one minute as being personal use.

In order to confirm which person used the personal computer to access a particular website, the auditors reviewed the internet cookies⁴, browser favorites⁵, and temporary internet files⁶ for each computer. If Windows NT or Windows 2000 was the operating software for a personal computer, then all of the above could be used to identify the computer user. If Windows 95 was the operating system, then only internet cookies could be attributed to a specific employee.

Once the auditors completed their analysis of website access, they referred their reports to managers and supervisors in the various regions of the State in order for those managers and supervisors to make final determinations of the identity of the employee using a particular personal computer from April 8th to April 14th, 2002.

Several feet away from Grievant's workstation is a personal computer with access to the internet. The computer's operating system is Windows 95. If Grievant logs into the Agency intranet but steps away from the computer, a second employee can use the computer to access the internet without having to log off Grievant. When the second employee uses the internet for personal use, that use is attributed to the IP address associated with Grievant. The practice at the Facility was for the Traffic Controller to log onto the computer at the beginning of his shift but not log off until the end of the shift or even later when someone else logged the Traffic Controller off of the computer.

During the review week, Grievant remained logged onto the Agency's internet during his shift even though he was not always using the computer during that shift. Several other employees used the computer while Grievant returned to his duties. Grievant was not away from his work station for more than two hours, according to the Facility Manager, because Grievant's supervisor would have noticed Grievant's absence for that period of time. The other employees using the internet for personal use were acting in accordance with the instructions from the former Facility Manager. When the Agency installed a new internet based communications system, the former Facility Manager encouraged employees to use the internet for personal use in order to become familiar with the internet.

Grievant's IP address had a total record count of 70,853 for the review week. His highest scoring day was April 11, 2002 with a record count of 27,787. Grievant used a

⁴ When a computer user accesses some websites, a website may transfer a record onto the user's personal computer to identify that user. The website can use the cookie to track each time the user returns to that website or to other websites.

⁵ A computer user may use his or her browser to make a list of the websites he or she most frequently wishes to access.

⁶ The Temporary Internet Files folder is the location on the hard drive of a personal computer where Web pages and files (such as graphics) are stored as the user views them. This speeds up the display of pages that have already been accessed because a browser can open them from the computer's hard drive instead of reloading them from the internet.

password to log onto his personal computer and the Agency's network at 0:23 a.m. and the two hour cap was reached by 3:15 a.m. Grievant's IP address accessed numerous non-business related websites. He logged off the computer at 11:59 p.m.

CONCLUSIONS OF POLICY

Unacceptable behavior is divided into three types of offenses, according to their severity. Group I offenses "include types of behavior least severe in nature but which require correction in the interest of maintaining a productive and well-managed work force." DHRM § 1.60(V)(B).⁷ Group II offenses "include acts and behavior which are more severe in nature and are such that an additional Group II offense should normally warrant removal." DHRM § 1.60(V)(B)(2). Group III offenses "include acts and behavior of such a serious nature that a first occurrence should normally warrant removal." DHRM § 1.60(V)(B)(3).

DHRM Policy 1.75 governs State employee use of the internet.⁸ This policy provides:

Certain activities are prohibited when using the Internet or electronic communications. These include, but are not limited to:

- accessing, downloading, printing or storing information with sexually explicit content as prohibited by law (see Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001);
- downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;
- installing or downloading computer software, programs, or executable files contrary to policy;
- uploading or downloading copyrighted materials or proprietary agency information contrary to policy;
- uploading or downloading access-restricted agency information contrary to policy or in violation of agency policy;
- sending e-mail using another's identity, an assumed name, or anonymously;

⁷ The Department of Human Resource Management ("DHRM") has issued its *Policies and Procedures Manual* setting forth Standards of Conduct for State employees.

⁸ The Agency adopted a policy IT-98 in accordance with Executive Order 51(99) governing use by VDOT employees. VDOT IT-98 creates a zero tolerance for personal use of the internet. State agencies are entitled to draft policies that vary from DHRM Policy 1.75 as long as those policies are consistent with DHRM Policy 1.75. VDOT IT-98 is contrary to DHRM Policy 1.75 because the Agency's policy sets a zero tolerance standard for personal use while the DHRM policy allows incidental and occasional use. To the extent the Agency's policy is not in accordance with DHRM policy, it is not enforceable. Thus, the Hearing Officer will analyze this case using DHRM Policy 1.75.

- permitting a non-user to use for purposes of communicating the message of some third party individual or organization;
- any other activities designated as prohibited by the agency.

DHRM Policy 1.75 permits State employees to use the internet for personal use within certain parameters as follows:

Personal use means use that is not job-related. In general, **incidental and occasional** personal use of the Commonwealth's Internet access or electronic communication systems is permitted; however, personal use is prohibited if it:

- interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;
- adversely affects the efficient operation of the computer system;
- violates any provision of this policy, any supplemental policy adopted by the agency supplying the Internet or electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law. (See Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001.) (Emphasis added).

An employee making personal use of the internet for over two hours has violated DHRM Policy 1.75. The question in this grievance is not whether excessive use occurred, but whether Grievant is the one who engaged in that excessive use. The Hearing Officer finds that the Agency has not met its burden of proof to show that Grievant is the person responsible for two hours of personal use of the internet.

Grievant logged on at 0:23 a.m. and the two hour threshold was reached at 3:15 a.m., approximately 3 hours later. If Grievant was the person engaging in personal use during that time, it would mean that he had left his workstation and was sitting at the personal computer for a lengthy continuous period of time. While investigating this grievance, the Facility Manager spoke with Grievant's supervisor, who the Facility Manager considered a "by the book supervisor". According to the supervisor, who sits right behind Grievant, the supervisor would have noticed if Grievant was away from his workstation for an extended period of time. The supervisor did not recall Grievant being away from his workstation for an extended period of time during the review week. Had Grievant been away from his workstation for an extended period of time, the supervisor would have counseled or disciplined Grievant for doing so.

It is likely that other employees engaged in personal use of the internet while Grievant was logged on to the computer for several reasons. First, Grievant did not work a 24 hours shift but he was logged onto the computer for approximately 24 hours on April 11, 2002. This fact supports Grievant's testimony that the Facility practice was

for a Traffic Controller to log on to the intranet but not log off before other employees began using the internet. Second, the former Facility Manager encouraged employees to use the internet for personal use in order to become proficient when using the Agency's internet-based monitoring system. This fact suggests some employees may have mistaken the former Facility Manager's instruction to engage in personal use of the computer as permission to continue using the internet for personal use once the new communication system was in operation. Third, Grievant presented evidence of other employees who engaged in personal use of the internet. Forth, the computer's cookie folder showed cookies under the names of several employees confirming that the Grievant's computer was used by many employees.

Based on the evidence presented, the Hearing Officer concludes that Grievant is not the person solely responsible for the personal⁹ internet use attributed to him. Although Grievant admits to some personal use of the internet¹⁰, no evidence was presented showing how much use was admitted by Grievant. Thus, the evidence is insufficient for the Hearing Officer to conclude that Grievant's use of the internet exceeded incidental and occasional personal use. The disciplinary action against Grievant must be rescinded.

DECISION

For the reasons stated herein, the Agency's issuance to the Grievant of a Group II Written Notice of disciplinary action with suspension is **rescinded**. The Agency is directed to provide the Grievant with **back pay** for the period of suspension less any interim earnings that the employee received during the period of suspension and credit for annual and sick leave that the employee did not otherwise accrue. GPM § 5.9(a)(3). DHRM Policy No. 1.60(IX)(B)(2).

APPEAL RIGHTS

You may file an administrative review request within **10 calendar** days from the date the decision was issued, if any of the following apply:

1. If you have new evidence that could not have been discovered before the hearing, or if you believe the decision contains an incorrect legal conclusion, you may request the hearing officer either to reopen the hearing or to reconsider the decision.
2. If you believe the hearing decision is inconsistent with state policy or agency policy, you may request the Director of the Department of Human Resource Management

⁹ Several websites were in foreign languages. No evidence was presented suggesting Grievant knew how to read those languages.

¹⁰ Grievant admitted to accessing certain sites, but the Agency did not present evidence of the amount of time Grievant spent at those sites.

to review the decision. You must state the specific policy and explain why you believe the decision is inconsistent with that policy.

3. If you believe that the hearing decision does not comply with the grievance procedure, you may request the Director of EDR to review the decision. You must state the specific portion of the grievance procedure with which you believe the decision does not comply.

You may request more than one type of review. Your request must be in writing and must be **received** by the reviewer within 10 calendar days of the date the decision was issued. You must give a copy of your appeal to the other party. The hearing officer's **decision becomes final** when the 10-calendar day period has expired, or when administrative requests for review have been decided.

You may request a judicial review if you believe the decision is contradictory to law. You must file a notice of appeal with the clerk of the circuit court in the jurisdiction in which the grievance arose within **30 days** of the date when the decision becomes final.¹¹

[See Sections 7.1 through 7.3 of the Grievance Procedure Manual for a more detailed explanation, or call EDR's toll-free Advice Line at 888-232-3842 to learn more about appeal rights from an EDR Consultant].

Carl Wilson Schmidt, Esq.
Hearing Officer

¹¹ Agencies must request and receive prior approval from the Director of EDR before filing a notice of appeal.