Issue: Group I Written Notice (failure to comply with established written policy); Hearing Date: 6/5/07; Decision Issued: 6/9/07; Agency: VDOT; AHO: Lorin A. Costanzo, Esq.; Case No. 8609; Outcome: Agency upheld in full.

Commonwealth of Virginia
Virginia Department of Transportation

DECISION OF HEARING OFFICER

In re: Grievance Case No. 8609

Hearing Date: June 5, 2007
Decision Date: June 9, 2007

PROCEDURAL HISTORY

On January 29, 2007, Grievant was issued a Group I Written Notice for failure to comply with established written policy; failure to maintain the conditions of security (including safeguarding of passwords) in violation of DHRM Policy # 1.75, Use of Internet and Electronic Communication Systems.[1] On February 26, 2007, Grievant timely filed a grievance to challenge the disciplinary action. The grievance proceeded through the resolution steps and when the parties failed to resolve the grievance the agency head qualified the grievance for a hearing.[2] On May 10, 2007, Department of Employment Dispute Resolution assigned this grievance to the Hearing Officer. On June 5, 2007, a hearing was held at Agency's district office.

APPEARANCES

Grievant (also testified as witness)
Admin. Specialist
Transportation Manager
Retiree
Agency Advocate
Agency Party Designee (also testified as a witness)
IT Manager

ISSUES

Were the Grievant's actions such as to warrant disciplinary actions under the Standards of Conduct? If so, what was the appropriate level of disciplinary action for the conduct at issue?

[1] Agency Exhibit 2. and Grievant Exhibit B. Written Notice issued January 29, 2007.
[2] Agency Exhibit 2. and Grievant Exhibit B. Grievance Form A, filed February 26, 2007.

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. [3] A preponderance of the evidence is evidence which shows that what is intended to be proved is more likely than not; evidence that is more convincing that the opposing evidence.[4]

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 (VDOT) employs Grievant as a Manager. He has been employed approximately nine years by the Agency. No evidence of prior disciplinary action against Grievant was presented and Agency stipulated at hearing that there are no issues with computer use other than what is at issue in the present grievance hearing. Grievant's supervisor testified Grievant has a good working relationship and is considered a very good employee of VDOT.

The Commonwealth of Virginia's policy on Use of the Internet and Electronic Communications Systems provides that when using the Commonwealth's Internet access or electronic communications, equipment and capability, individuals must use the Internet or electronic communications only in accordance with State and agency policy and maintain the conditions of security (including safeguarding of passwords) under which they are granted access to such systems.[5]

VDOT policy provides that the VDOT computer system is for the use of authorized users only and defines "user" as anyone with access to VDOT's Information Technology Resources, which includes all VDOT personnel and contractors. Users are further charged with responsible for the adequate protection of VDOT Information Technology Resources within their control or possession and all employees of the Department are responsible for the protection of technology resources and data within their control or possession. This policy also states VDOT has the right to monitor any and all aspects of its computer system at any time, without notice and anyone using this system expressly consents to such monitoring.[6]

---

[3] Section 5.8, Department of Employment Dispute Resolution, Grievance Procedure Manual, effective August 30, 2004.

[4] Section 9, Department of Employment Dispute Resolution, Grievance Procedure Manual, effective August 30, 2004.

[5] Agency Exhibit 4. And Grievant's Exhibit D. Department of Human Resources Management ("DHRM")Policy No. 1.75, *Use of Internet and Electronic Communications*, effective August 1, 2001.

[6] Agency Exhibit 3, page 3 & 4. VDOT Policy I, *Personnel Security*.

Agency policy further establishes that passwords are mandatory for all user accounts that access sensitive VDOT IT assets (e.g., network, servers, Desktop, applications, data, etc.) and passwords are confidential, should not be written down, and should not be shared with anyone. [7]

Grievant supervised Retiree prior to Retiree's retirement from VDOT on 9/24/06 after 40+ years of service. Retiree left service with VDOT to go to work for a contractor of VDOT. His retirement date was 9/24/06. However, his last work day was 9/22/06. On 9/22/06 Retiree was not able to complete two employee work performance evaluations in part related to a computer slow down and other computer problems. Grievant and Retiree agreed to a return on October 2, 2006 to complete the evaluations.

Following Retiree's retirement date Grievant requested Information Technology ("IT") reactivate Retiree's VDOT computer network account so that Retiree could use it. A number of e-mails were transmitted relating to Grievant's request to reactivate Retiree's computer network account for Retiree's utilization on 10/2/06:

1. 4:50 P.M. on 9/28/06 … IT Manager e-mailed Grievant concerning Grievant's request to reactivate Retiree's VDOT computer network account so that Retiree could use it on 10/2/06. Grievant was informed their records indicated Retiree left state service as of 9/24/06 and if this is correct they can not activate Retiree's account without additional guidance/approval "since he is no longer an employee of the Commonwealth".

2. 9/28/06 … Grievant requested IT Manager open Retiree's computer network account to Grievant as Retiree's Supervisor. Grievant indicated he will review the data and notify IT Manager when to close and delete the account.

3. 8:11 A.M. on 9/29/06 … IT staff e-mailed Grievant that she had reinstated Retiree's computer network account, that Grievant will need to call her for the password and that he needed to let her know after he had reviewed matters so she can disable the network logon.

4. 10:23 A.M. on 9/29/06 … District Human Resources Manager indicated to Residency Administrator her "over riding concern is that Grievant even asked for Retiree to have access when he clearly is no longer a State employee". She indicated she would have expected Grievant, as a manager, to be aware this is inappropriate and further expressed concern that Retiree not get such access by Grievant giving it to him.

5. 10:45 A.M. on 9/29/06 … Residence Administrator indicated to District Human Resources Manager he believe she misunderstood the reason for Grievant's request. He believed the intent is not for Retiree to have access to the account but for Grievant to retrieve things from Retiree's account.

[7] Agency Exhibit 3, page 5. *Password Management - Logical Access Control.*

6. 10:46 A.M. on 9/29/06 ... Grievant e-mailed IT indicating he will complete the review next week and advise so the network logon can be closed and disabled.

7. 11:03 A.M. 9/29/06 … Grievant e-mailed that Retiree was coming by Monday morning, please call me then and we will finish up with the items they could not do last Friday because of computer issues.

8. 11:41 A.M. on 9/29/06 … In an e-mail to Residency Administrator the District Human Resources Manager noted the issue was not whether Grievant can have access to a subordinate employee's account but whether a former employee can have access in the computer account. The District Human Resources Manager expressed that in the initial request it seemed clear that Grievant wanted Retiree to have access to the computer account and when the initial request was denied Grievant modified his request. Grievant's modified request was to access Retiree's account in Grievant's supervisory capacity. It was this modified request that was considered consistent with policy and IT completed the request by providing to Grievant the password. [8]

Prior to October 2, 2006 Grievant was specifically informed that Retiree could not have access to the network computer account after retirement from VDOT. The email of 4:50 P.M. on 9/28/06 provided specifically IT could not activate the computer network account due to Retiree no longer being an employee of the Commonwealth.

Grievant was informed by IT that it was policy to lock down the computer network account of an employee leaving service on the last day of employment but a departing employee's supervisor can get access to the computer network account of the subordinate in order to review data for use by VDOT. After this review IT would close and delete the computer network account.

Grievant was informed on 9/28/06 by IT that since Retiree had left state service his account could not be reactivated for Retiree to access without special approvals.[9] He then requested the Retiree's computer network account be reactivated for Grievant's access as a supervisor of an employee leaving service. At this second request by Grievant the Retiree's computer network account had been reinstated for Grievant's use and Grievant was instructed to call IT for the password.

On 10/2/06 Grievant met Retiree at AHQ and after a call to IT Grievant signed Retiree onto Retiree's computer network account using a password and logon IT provided Grievant. The logon and password to activate Retiree's computer network account was not the same logon and password for Grievant's computer network account. Grievant wrote down the password, left it with Retiree, then left Retiree unsupervised and returned to the Residency to pursue other matters. Grievant allowed Retiree to have the password

[8] Agency Exhibit 2. and Grievant's Exhibit B. pages 15-33 through 18-33. Copies of E-mails.

[9] Agency Exhibit 2. and Grievant's Exhibit B. -pages 21-33 & 22-33. Document of Grievant.

given to him, and allowed Retiree unsupervised access to the computer network account for Retiree to complete certain business related matters. It was subsequently determined that the computer network account was utilized to access non-business related websites.

The Agency electronically monitors computer logon/log off activities and site activities. Grievant's and Retiree's account were reviewed and it was noted that Grievant's account was accessed (by entering a password at 9:32 A.M. on 10/2/06) in the Residency while Retiree's computer account was accessed (by entering a password on 10/2/06 at 9:39 A.M.) in the AHQ. The distance between the Residency and the AHQ was estimated to be approximately 12 to 15 miles apart, making it virtually not possible for Grievant to log on to both computers at these separate locations within seven minutes of each other.

IT Manager was aware that Retiree's computer account was disabled and access given to a supervisor to review matters on e-mail and net access drives. The logon/log activities and site visited information ultimately led to contact with the office of the Inspector General and an investigation being initiated 10/13/06 concerning the computer access and related matters. The investigative report of the incident was received by the Agency in December of 2006.

The parties stipulated that Grievant does not have a reputation for excessive personal use of a VDOT computer and that Grievant has closed out a number of employees of VDOT.

Grievant has received MOAT training stressing passwords should never be shared and should always be kept confidential. On October 26, 2005 Grievant completed Security Awareness Training administered through MOAT.[10]

Grievant signed an Information Technology Security Access Agreement (Form, ISD-33B Rev. 11/98 tgn). This Agreement provided, "Logon-id's and passwords are not to be shared among personnel. No one is allowed to give their logo-id/password to another person."[11]

CONCLUSIONS OF LAW AND POLICY

The General Assembly enacted the Virginia Personnel Act, Va. Code Section 2.2-2900 et seq., establishing the procedures and policies applicable to employment within the Commonwealth of Virginia. This comprehensive legislation includes procedures for hiring, promoting, compensating, discharging, and training state employees. It also provides for a grievance procedure. The Act balances the need for orderly administration

[10] Agency Exhibit 3. Certificate, Security Awareness Training administered through MOAT.

[11] Agency Exhibit 3, page 8 & 9. Information Technology Security Access Agreement .

of state employment and personnel practices with the preservation of the employee's ability to protect his rights and pursue legitimate grievances. These dual goals reflect a valid governmental interest in and responsibility to its employees and workplace. *Murray v. Stokes*, 237 Va. 653, 656 (1989).

Code Section 2.2-3000(A) sets forth the Virginia grievance procedure and provides, in part:

> "It shall be the policy of the Commonwealth, as an employer, to encourage the resolution of employee problems and complaints .... To the extent that such concerns cannot be resolved informally, the grievance procedure shall afford an immediate and fair method for the resolution of employee disputes which may arise between state agencies and those employees who have access to the procedure under Section 2.2-3001."

To establish procedures on Standards of Conduct and Performance for employees of the Commonwealth of Virginia and pursuant to Section 2.2-1201 of the Code of Virginia, the Department of Human Resource Management ("DHRM") promulgated the *Standards of Conduct, Policy No. 1.60, effective 9/16/93.* The *Standards of Conduct* provide a set of rules governing the professional and personal conduct and acceptable standards for work performance of employees. The *Standards* serve to establish a fair and objective process for correcting or treating unacceptable conduct or work performance, to distinguish between less serious and more serious actions of misconduct, and to provide appropriate corrective action.

Unacceptable behavior is divided into three groups according to the severity of the behavior. Group I are the least severe behaviors and Group II includes acts and behaviors which are more severe in nature and are such that an additional Group II offense should normally warrant removal.[12] The offenses set forth in Standards of Conduct Section V. "UNACCEPTABLE STANDARDS OF CONDUCT (OFFENSES)" are not all-inclusive, but are intended as examples of unacceptable behavior for which specific disciplinary actions may be warranted. Accordingly, any offense that, in the judgment of agency heads, undermines the effectiveness of agencies' activities, may be considered unacceptable and treated in a manner consistent with the provisions of Section V.[13]

The Agency has shown and Grievant has admitted that on October 2, 2006, he met with Retiree, obtained access to Retiree's past computer network access account, wrote down the password, and allowed Retiree to have the password when he left Retiree alone at AHQ and went to a different facility.

Grievant asserts and the Agency does not contradict that Grievant only provided

[12] Agency Exhibit 5. and Grievant's Exhibit C. *Section* (V)(B), Department of Human Resources Management Policies and Procedures Manual, Policy No. 1.60, effective date 9/16/93.

[13] Agency Exhibit 5. and Grievant's Exhibit C. *Section* (V)(A), Department of Human Resources Management Policies and Procedures Manual, Policy No. 1.60, effective date 9/16/93.

to Retiree the password that accessed Retiree's computer network account and Grievant did not provide to Retiree Grievant's personal logon and password. Grievant further contends that as he kept his personal logon and password confidential he was, to the best of his belief, in compliance with policy.

Grievant does not contest the two 9/28/06 e-mails referenced above. The first e-mail informed Grievant that if Retiree had left state service they could not activate Retiree's computer network account without additional guidance/approval since he is no longer an employee. The second e-mail was Grievant's request to open Retiree's computer network account to Grievant as Retiree's supervisor.

Grievant has received training on Policy and Security concerns with IT Systems and password protection. Annual training has been conducted with Grievant emphasizing the security of IT Systems. Grievant had, prior to October 2, 2006, completed required computer security training that stated policy did not allow a non-employee computer access and that policy did not allow sharing passwords. Agency policy established requirements that users will not write their passwords down or store it on their computer and must not share their passwords with anyone. Grievant received training through MOAT as to Information Security Best Practices which specifically provides, "Passwords are one of the first layers of protection and passwords should never be shared and should always be kept confidential.

Grievant had been told Retiree should not be given access to the computer network account. Policy clearly requires password protection be given to the password Grievant received, as Retirees supervisor, to access Retiree's computer network account. The password should not have been shared and doing so violated established policy. Retiree should not have been given computer network access on Grievant's sole discretion and doing so violated established policy.

Grievant contends per VDOT Policy I which provides in part, *"The VDOT computer system is for the use of authorized users only. Users are anyone with access to VDOT's Information Technology Resources, which included all VDOT personnel and contractors."* that it was acceptable, or at least unclear, if Retiree could access the password and computer network account on October 2, 2006. However, *VDOT Policy I* clearly states that the VDOT computer system is for the use of **authorized users only** and further, as testimony at hearing indicated, not all contractors are authorized computer access.

Grievant also contends that for the Agency even to have initially considered a Group II was improper, too severe, and violates policy. Grievant contends that issuing a Group I Written Notice on 1/29/07 for an offense date of October 2, 2006 was not timely and violates policy. He contends that he has received counseling which was sufficient action on the part of management and therefore the action of issuing a Group I Written

Notice is repetitive and improper.[14]

In reviewing agency-imposed discipline, the hearing officer must give due consideration to management's right to exercise its good faith business judgment in employee matters, and the agency's right to manage its operations.[15] Policy does not preclude both counseling and disciplinary action nor does policy require an election of only one be made. DHRM Policy 1.60 (VI) (B), indicates the following are possible corrective actions:

1. referral to the employee assistance program or other professional assistance;
2. counseling; ***and/or***
3. disciplinary action. *(emphasis added)*

Management should issue a Written Notice as soon as possible after an employee's commission of an offense.[16] But this cannot be construed to negate the duty of management to investigate thoroughly and determine the facts prior to determining if an offense has occurred and what action, if any, would be appropriate under the circumstances. The timeline of events outlined in the Report of Investigation (Agency Exhibit 2) and testimony indicate that on:

1. October 13, 2006 … The Investigation Division was contacted by management.
2. October 25, 2006 … Grievant was interviewed by investigator.
3. October 26, 2006 … Grievant provided the Investigation Division a written statement.
4. November 2, 2006 … Re-interview was conducted with Grievant.
5. November 6, 2006 … Grievant provided a subsequent e-mail statement.
6. December of 2006 … Report of Investigation received by Agency prior to the Holidays.
7. January 19, 2007… Grievant sent e-mail advance notice of intent to issue a Group I.
8. January 19, 2007... Group I Written Notice issued.

This timeline indicated that the time between the alleged event and the disciplinary action issuing is not inconsistent with policy. The Agency acted in a timely manner, appropriately, and its actions were consistent with policy in the issuance of the Group I Written Notice on January 29, 2007 for the offense of October 2, 2006.

Grievant further raised concerns that on the day of the issuance of Written Notice (i.e. 1/29/07) he asked for but was not granted additional time to submit information. Agency testimony indicated that on January 19th, 2007, advance notice of the intent to issue a Group I was given Grievant and Grievant submitted a number of documents which the Agency considered together with the investigative report prior to issuing the Group I Written Notice. The Agency initially had concerns that nature of the offense rose to a Group II for "Failure to follow a supervisor's instructions, perform assigned work, or otherwise comply with established written policy" which is set forth as an example of unacceptable behaviors per Group II Offenses under the Standards of Conduct.[17] The

[14] Grievant Exhibit B 31-33 & Agency Ex. 2, 361-33. E-mail of 1/19/07; testimony.

[15] Dept. of Employment Dispute Resolution, Rules for Conducting Grievance Hearings, Section VI. B.

[16] Agency Exhibit 5. and Grievant's Exhibit C. DHRM Policy No. 1.60 effective date of 9/16/03, Standards of Conduct, Section VII. B. 1.

[17] Agency Exhibit 5. and Grievant's Exhibit C. Agency Exhibit 5. DHRM Policy No. 1.60, effective

normal disciplinary action for a Group II offense is issuance of aWritten Notice only, or a Written Notice and up to ten workdays of suspension without pay.[18]

The *Standards of Conduct* provides that while disciplinary actions imposed shall not exceed those set forth in this policy for specific offenses, agencies may reduce the disciplinary action if there are mitigating circumstances, such as:

a. conditions that would compel a reduction in the disciplinary action to promote the interests of fairness and objectivity; or
b. an employee's long service or otherwise satisfactory work performance.[19]

The Agency took into consideration mitigating circumstances and also took into consideration the strong concerns, expressed in policy and in practices, in maintaining security, protecting passwords, and limiting access to their computer system. Consideration of mitigating circumstances influenced the Agency decision not to issue a Group II Written Notice (with or without a suspension for up to ten workdays). Consideration of mitigating circumstances, including the Grievant's very good work history over his 9 years of service, influenced the Agency decision to issue a Written Notice for a Group I Offense and not a Group II Offense.

Under the *Rules for Conducting Grievance Hearings*, Section VI, B, 1, a hearing officer must give deference to the agency's consideration and assessment of any mitigating and aggravating circumstances. Thus, a hearing officer may mitigate the agency's discipline only if, under the record evidence, the agency's discipline exceeds the limits of reasonableness. The Agency's discipline did not exceed the limits of reasonableness.

Upon reviewing the facts de novo (afresh and independently, as if no determinations had yet been made) it is determined that (i) Grievant engaged in the behavior described in the Written Notice; (ii) The behavior constituted misconduct; (iii) the Agency's discipline was consistent with law and policy; and (iv) there are no mitigating circumstances to justify a reduction or removal of the Group I disciplinary action. The Agency has proven by a preponderance of the evidence that the disciplinary action of issuing a Group I Written Notice was warranted and appropriate under the circumstances.

DECISION

For the reasons stated herein, the Agency's issuance of a Group I Written Notice of disciplinary action is UPHELD.

9/16/93, Section (V)(B)(2)(a).

[18] Agency Exhibit 5. and Grievant's Exhibit C. DHRM Policy No. 1.60, effective 9/16/93, Section (VII)(D(2).

[19] Agency Exhibit 5. and Grievant's Exhibit C. DHRM Policy No. 1.60, effective 9/16/93, Section (VII)(C)(1).

APPEAL RIGHTS

As the Grievance Procedure Manual sets forth in more detail, this hearing decision is subject to administrative and judicial review. Once the administrative review phase has concluded, the hearing decision becomes final and is subject to judicial review.

Administrative Review: This decision is subject to three types of administrative review, depending upon the nature of the alleged defect of the decision:

1. **A request to reconsider a decision or reopen a hearing** is made to the hearing officer. This request must state the basis for such request; generally, newly discovered evidence or evidence of incorrect legal conclusions are the basis for such a request.

2. **A challenge that the hearing decision is inconsistent with state policy or Agency policy** is made to the Director of the Department of Human Resources Management. This request must cite to a particular mandate in state or Agency policy. The Director's authority is limited to ordering the hearing officer to revise the decision to conform it to written policy. Requests should be sent to:

   Director, Department of Human Resources Management
   101 N. 14th Street, 12th Floor
   Richmond, Virginia 23219

3. **A challenge that the hearing decision does not comply with grievance procedure** is made to the Director of EDR. This request must state the specific requirement of the grievance procedure with which the decision is not in compliance. The Director's authority is limited to ordering the hearing officer to revise the decision so that it complies with the grievance procedure. Requests should be sent to:

   Director, Department of Employment Dispute Resolution
   830 East Main St., Suite 400
   Richmond, VA 23219.

A party may make more than one type of request for review. All requests for review must be made in writing, and received by the administrative reviewer, within **15 calendar days** of the date of the original hearing decision. (Note: the 15-day period, in which the appeal must occur, begins with the date of issuance of the decision, not receipt of the decision. However, the date the decision is rendered does not count as one of the 15 day following the issuance of the decision is the first of the 15 days.) A copy of each appeal must be provided to the other party.

A hearing officer's original decision becomes a **final hearing decision**, with no further possibility of an administrative review, when:

1. The 15 calendar day period for filing requests for administrative review has expired and neither party has filed such a request; or,

2. All timely requests for administrative review have been decided and, if ordered by EDR or DHRM, the hearing officer has issued a revised decision.

Judicial Review of Final Hearing Decision: Within **thirty days** of a final decision, a party may appeal on the grounds that the determination is contradictory to law by filing a notice of appeal with the clerk of the circuit court in the jurisdiction in which the grievance arose. You must give a copy of your notice of appeal to the Director of the Department of Employment Dispute Resolution. The agency shall request and receive prior approval of the Director before filing a notice of appeal.

_____

Lorin A. Costanzo, Hearing Officer