Issue: Group III Written Notice with termination (violating security practices and protocol, undermining IT communication activities and programs); Hearing Date: 09/17/03; Decision Issued: 09/26/03; Agency: DMV; AHO: Carl Wilson Schmidt, Esq.; Case No. 5801; **Administrative Review: HO Reconsideration Request received 10/06/03; Reconsideration Decision issued 10/24/03; Outcome: No newly discovered evidence or incorrect legal conclusions; Administrative Review: EDR Ruling Request received 10/06/03; EDR Ruling issued 12/29/03 [2003-440]; Outcome: HO neither abused his discretion nor exceeded his authority; Administrative Review: DHRM Ruling Request received 10/06/03; DHRM Ruling issued 02/11/04; Outcome: HO's decision comports with provisions of DHRM Policy 1.60. Will not interfere with decision.**

COMMONWEALTH of VIRGINIA

Department of Employment Dispute Resolution

DIVISION OF HEARINGS

DECISION OF HEARING OFFICER

In re:

Case Number: 5801

Hearing Date: September 17, 2003
Decision Issued: September 26, 2003

PROCEDURAL HISTORY

On June 3, 2003, Grievant was issued a Group III Written Notice of disciplinary action with removal for:

> *Safe, reliable, and secure computer Network Systems are essential to the effective operations of the Agency. Employee was computer systems senior engineer. He formerly worked on in LAN/Network Security and after certain access rights were removed by Network Security, system records show he knowingly and intentionally reinstated those rights and gave certain access rights to others, thereby violating the security practices and protocol in which he had been trained and certified. This resulted in undermining the Agency's IT communication activities and programs.*

On June 5, 2003, Grievant timely filed a grievance to challenge the Agency's action. The outcome of the Third Resolution Step was not satisfactory to the Grievant and he requested a hearing. On August 27, 2003, the Department of Employment Dispute Resolution assigned this appeal to the Hearing Officer. On September 17, 2003, a hearing was held at the Agency's regional office.

APPEARANCES

Grievant
Grievant's Counsel
Agency Party Designee
Agency Representative
Five witnesses

ISSUE

Whether Grievant should receive a Group III Written Notice of disciplinary action with removal.

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 Department of Motor Vehicles employed Grievant as a Computer Systems Senior Engineer until his removal on June 3, 2003.[1] Grievant had been working with Network Systems Support Group (NSS)[2] but was moved to a new position[3] sometime at the beginning of 2003. The purpose of his new position was:

> Provides technical support to the Zenworks Administrator in the areas of monitoring of DMV pcs to ensure appropriate client software and appropriate pc naming conventions are utilized. In addition, provide support to the Zenworks Administrator to make sure appropriate logging/monitoring reports are run in a timely manner to make sure

[1] Grievant worked for the Agency for approximately 17 years.

[2] NSS typically refers to Novell Storage System but can be used to refer to those staff with responsibility for administering and maintaining the Novell network and infrastructure.

[3] Once the responsibilities of Grievant's new position were finalized, Grievant no longer had responsibility for checking security on the Novell network.

application objects are properly moved from the test to production environment and that the inventory monitoring function is working properly.[4]

The Agency has numerous offices throughout the Commonwealth and maintains records regarding customers, employees, and Agency operations in various computer databases. The Agency uses state-of-the-art Novell Netware software to create a Local Area Network (LAN) to efficiently structure and utilize its databases. Novell Directory Services (NDS) provides a logical tree-structure[5] of all resources on the LAN so that computer users can access them without necessarily knowing where those resources are physically located.

When an employee working in a remote location in the State requires technical assistance with a personal computer, Agency IT staff can access that employee's computer from the Agency's Central Office. Novell Zenworks Remote Control software allows IT staff to access the employee's personal computer as if the IT person was sitting in front of the employee's computer even though the IT person is actually working from the Agency's Central Office. Before Central Office IT staff can access an employee's personal computer, the employee must give permission to do so and must be present during the session. Remote-control sessions are documented by the creation and processing of a support ticket.

All DMV employees are given a password-protected user account to enable them to access the LAN. Employees working in the Information Technology division of the Agency are given additional accounts depending upon their duties.

DMV NDS Security Design policy states, "Where possible rights will be assigned at the highest possible level in the tree and allowed to flow down."[6] Employees are given only the minimum access rights necessary to do their jobs. For example, if the Agency creates a workgroup to accomplish a specific task, the Agency creates an organization unit on the network and gives that unit certain access rights. Employees assigned to work within that unit receive the same access rights assigned to the unit on the network. As employees move into and out of the workgroup, their rights are added or deleted with the move because their network access rights flow down from the workgroup.

---

[4] Agency Exhibit 10.

[5] Directory services are databases of information for storing, accessing, managing, and using different kinds of information about users and resources in a computing environment. Novell Directory Services (NDS) is an object-oriented implementation of directory services that allows one to build sophisticated naming schemes and databases across network-wide resources. The NDS architecture provides global access to all the network resources regardless of their physical location, forming a single information system.

[6] Agency Exhibit 2.

On April 1, 2003, Grievant's ADMIN account access rights were reduced by Agency managers. On April 3, 2003, Grievant realized his rights had been reduced. NSS created the Desktop Management Services (DMS) container and ZENADMIN role[7] on April 3, 2003. On April 7, 2003, NSS put Grievant's ADMIN account in the ZENADMIN role. Grievant's personal account was placed in the DMS container. On April 8, 2003, Grievant used his ADMIN account to grant ZENADMIN role full rights to HQ[8] and FIELD. Grievant notified others in the Agency that he had his rights back, meaning that the rights he had in his current position were similar to the rights he had in his former position in NSS.

Another employee, Mr. BJ, had an ADMIN account in the in DMS container. His access rights should have been the same as Grievant's. When Grievant claimed to have been restored full rights, the IT Manager audited Mr. BJ's access rights and concluded that Grievant had incorrectly claimed to have access rights he did not have. The IT Manager attended a conference located away from the Agency and was unable to immediately audit Grievant's account.[9]

On April 11, 2003, Grievant made changes to the TAPE[10] object. On April 17, 2003, Grievant created a new account called AATESTSEC. On April 21, 2003, Grievant used his ADMIN account to put the AATESTSEC account, Mr. BJ's personal account, and Grievant's personal account into ZENADMIN role. By doing so, Grievant granted these three accounts the same access rights available to the ZENADMIN role.

In September 2002, Grievant created an account called DMV456 to be used for testing. On April 22, 2003, Grievant enabled that account to bypass Remote Control settings. This change would enable Grievant to remotely control employees' computers without their knowledge. Grievant could take any action a computer user could take, (such as sending an email using GroupWise), without the user or anyone else knowing what happened and without the Agency being able to have an audit trail showing what happened.

On April 24, 2003, the IT Manager realized that the ZENADMIN roll had full access rights to HQ and FIELD and that Grievant's personal account was a trustee to HQ. She also discovered that Grievant's personal account, Mr. BJ's personal account, and the ATTESTSEC account were members of the ZENADMIN role. Most importantly, the IT Manager learned that Grievant's personal account had the security equivalent to

---

[7] "This role object is used to provide rights to administrator accounts for the purpose of administering the ZenWorks product." Agency Exhibit 6.

[8] The HQ object is an organizational unit containing "all the printer objects, server, and volume objects, ZenWorks policies, some NDS user groups, sub-containers for each administrative/work group and accounts used by applications." Agency Exhibit 6.

[9] The IT Manager was to return on April 28, 2003.

[10] The TAPE object has full access to the entire Novell Directory Service tree. The TAPE id is required to perform backups of the Agency's network databases.

TAPE. By having access to TAPE Grievant could change data stored in the Agency's back up systems.

By granting himself additional access rights, Grievant assumed what one witness called "God Access" over the Agency's databases. He jeopardized the integrity of the Agency's security procedures.

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).[11] 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 § 1.60(V) lists numerous examples of offenses. These examples "are not all-inclusive, but are intended as examples of unacceptable behavior for which specific disciplinary actions may be warranted. Accordingly, any offense which, in the judgement of agency heads, undermines the effectiveness of agencies' activities may be considered unacceptable and treated in a manner consistent with the provisions of this section."

When an employee changes positions within the Agency that employee's network access rights are not to be determined by the employee but by properly authorized Agency managers. In order to track changes to access rights, a form[12] is submitted for a newly reassigned employee. That form is intended to authorize to an employee only the network access rights necessary for the employee to complete his or her job. When Grievant was assigned to the ZenWorks project, he was given only the access rights necessary to complete his job.[13]

Grievant altered his access rights without permission from anyone. He subsequently granted himself "God Access" and was able to access any data within the network including the personal computers of Agency employees. Grievant could have copied or accessed personal information about Virginia drivers.

---

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

[12] The form is called a MISA61.

[13] Mr. BJ was given the same access rights and he found those rights to be adequate to complete his job.

DMV's Zenworks Remote Control Security Policy states, "Support staff shall not disabled the prompt to the end the user for establishing a remote management session." Agency support staff are required to sign a Remote Management Usage Agreement acknowledging, "Any access to a desktop (computer) without a support ticket is forbidden."[14] Grievant bypassed the Remote Control function thereby enabling him to operate employee personal computers without the employees being present and without any record of what was done.

Grievant changed his access rights in order to test what rights he had under the network while in his new position as a Zenworks administrator, and also to address a security concern he had identified in the network several month earlier.[15] Grievant attempted these tests without obtaining permission from the appropriate Agency managers and he conducted tests on a "live" part of the network. The Agency's practice was to require employees seeking to conduct tests to obtain approval for doing so and to create a "safe" area within the network to conduct tests so that if mistakes were made during testing, those mistakes would not harm other parts of the network.

Grievant is extremely intelligent and has demonstrated extensive knowledge of a complex computer network and the duties required of a systems expert. On the one hand, Grievant's individual skills and experience make him invaluable to the Commonwealth. On the other hand, given those same skills and experience, it is surprising Grievant did not realize the extent to which he placed the Agency's entire operations at risk. He took little precaution to protect the Agency from any mistakes he may have made while testing. He failed to notify Mr. BJ that Mr. BJ had "God Access" and could damage the network if any mistakes were made. The Agency believes that Grievant's failure to exercise appropriate judgment when coupled with the damage that Grievant could have caused renders Grievant unfit to work for the Agency. The Hearing Officer finds that the Agency has set forth sufficient facts to support its conclusion, and the issuance of a Group III Written Notice with removal is appropriate.

Grievant contends he had the authority to conduct necessary testing. This assertion is unfounded. Grievant's duties for checking for security concerns with the network had been removed when he assumed responsibilities under his new position. Grievant restored his rights before he raised questions with the IT Manager on April 9, 2003. His action to restore his rights was not with permission. When the IT Manager sent Grievant an email on April 10, 2003 stating, "Please try it again and let me know if you can still do the things you have listed below", her email was not an authorization to conduct a full testing procedure involving the entire network security system. Prior to sending the email, the IT Manager had conducted an audit to determine that Grievant could not have the rights he claimed. At best, she was asking Grievant to repeat what he had done prior to April 9th, and was not authorizing him to place the entire network at

[14] Agency Exhibit 3.

[15] Grievant's responsibilities for testing security problems within the network had been removed when he assumed his new duties with ZenWorks. He retained only limited NSS duties such as "the Magic database backup role and the Unix switch activity." Grievant Exhibit 3.

risk. Moreover, Grievant did not have permission to make the changes he made that gave rise to his April 9th email. Even if the IT Manager's email can be interpreted as an unlimited right to modify the network, Grievant's changes prior to April 9th remained unauthorized.

Grievant contends that the Agency retaliated against him, discriminated against him in order to prevent professional advancement, and violated his right of freedom of speech. No credible evidence was presented to support these allegations.

DECISION

For the reasons stated herein, the Agency's issuance to the Grievant of a Group III Written Notice of disciplinary action with removal is **upheld**.

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 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.[16]

[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

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

COMMONWEALTH of VIRGINIA

Department of Employment Dispute Resolution

DIVISION OF HEARINGS

DECISION OF HEARING OFFICER

In re:

Case No: 5801-R

Reconsideration Decision Issued: October 24, 2003

RECONSIDERATION DECISION

Grievance Procedure Manual § 7.2 authorizes the Hearing Officer to reconsider or reopen a hearing. "[G]enerally, newly discovered evidence or evidence of incorrect legal conclusions is the basis …" to grant the request.

Grievant raises numerous objections to the hearing decision. These points include (1) typographical errors[17], (2) restatement of facts originally rejected by the Hearing Officer as contrary to the evidence, and (3) restatement of arguments originally rejected by the Hearing Officer as unpersuasive. After considering these items, the Hearing Officer concludes that Grievant has not established a basis to reconsider the Agency's disciplinary action.

Grievant contends his responsibilities for working on the Novell network were not finalized because his EWP was not in final form. Grievant's work duties were finalized by Agency managers. Grievant was removed from the group controlling the network and moved to a unit designed to handle Zenworks. Grievant attempted to expand his work duties to include network security but the Agency resisted because it did not intend for Grievant to have network security responsibilities. Whether Grievant's EWP was put in final draft form is not significant.[18]

[17] For example, the hearing decision states Grievant worked for the Agency for 17 years but Grievant points out he worked there for four years and eight months. An opportunity for mitigation increases with the number of years worked. Because Grievant worked only for only four years and eight months, no mitigating circumstances exist based on the number of years worked.

[18] In Grievant's request for reconsideration he admits "I was only told to shift my full time focus to helping with the Zenworks projects."

Grievant objects to referring to Ms. KB as an IT manager. Because hearing decisions do not to refer to individuals by their names, the Hearing Officer selects titles to refer to individuals. Ms. KB was one of several people who "managed" the network. How individuals are referred to in the hearing decision does not affect the outcome of Grievant's case.

Grievant contends it is untrue that when he was assigned to the Zenworks project he was only given access rights necessary to do his job. Credible Agency testimony showed Grievant was not intended to have rights beyond those necessary to complete his duties in Zenworks.

Grievant contends that the DMV456 account only allowed him to remotely control the test account without prompting or knowledge. Credible Agency testimony showed that, irrespective of the account's name, Grievant was able to bypass Remote Control settings to remotely control employees' computers without their knowledge. Grievant's concern would not affect the outcome of the appeal.

Grievant contends that the Hearing Officer was misled into believing that there is a misa61 submitted to reflect the creation of a new department and Grievant's moving into the department. Credible Agency evidence showed that a misa61 form is used to assign access rights to employees. Grievant's assertion is incorrect.

Grievant asserts that would have been inappropriate for him to notify Mr. BJ that Mr. BJ had "God access" since it was his NSS team members who are responsible for addressing this problem.[19] The evidence showed, however, Grievant was not an NSS team member and that he granted himself the access rights. Grievant's assertion is unfounded.[20]

Grievant's objects to the Hearing Officer statement "When the IT managers sent Grievant an e-mail on April 10, 2003 stating 'Please try again let me know if you can still do the things you have listed below' her email was not an authorization to conduct a full testing procedure involving the entire network security system." Grievant states that the test only pertained to testing the security of the Novell NetWare. Grievant makes the Hearing Officer's point. Grievant was not authorized to test the entire network, his authorization was more limited.

Grievant objects to the Hearing Officer's statement "Even if the IT manager's e-mail can be interpreted as an unlimited right to modify the network, Grievant's changes prior to April 9 remain unauthorized." Grievant states that the changes prior to April 9th were to the FIELD and HQ containers. The time that changes were made is not as

[19] Grievant was disciplined for creating "God access"; he was not disciplined for failing to tell Mr. BJ of that access.

[20] Grievant was not disciplined for failing to notify Mr. BJ that Mr. BJ also had "God access." Grievant was disciplined for granting himself that level of access. Failing to notify Mr. BJ shows the damage that could have arisen because Grievant expanded his access level.

important as the nature of the changes made. Grievant may have modified objects associated with Zenworks, but the nature of his changes exceeded what was necessary for him to perform his duties within Zenworks. Grievant suggests there was nothing that said Grievant "is not to make changes in the NDS tree." In contrast, Grievant did not present any credible evidence suggesting he was authorized to make changes to the NDS tree that would affect areas beyond Zenworks.

Grievant states that assigning rights to the highest level of the tree and allowing them to flow down is not what needs to be done according to Zenworks administrator policies when working with the Zenworks product. Agency testimony showed it assigned rights from the top down. Whether doing so was what needs to be done is not as important as what was actually done.

Grievant suggests that Mr. BJ knew Grievant's ADMIN access rights were to be reduced but he and no one else in the Agency told Grievant before the rights were reduced on April 1, 2003. Whether or not Agency staff gave Grievant advance notice that his rights would be reduced is of little significance. If the Hearing Officer assumes for the sake of argument that the Agency's omission of notice was intentional, then the Agency's actions further support the conclusion that it did not want Grievant to have anything further to do with his former position and with network administration.

Grievant relies upon the testimony of Mr. BJ to support his contention that he was to have full administrative rights. Credible testimony of Ms. KB showed that it was never the Agency's intent to give Grievant full administrative rights. Ms. KB even audited Mr. BJ's access rights and concluded that Grievant had incorrectly claimed to have access rights that he did not have. Grievant subsequently expanded his rights.

Grievant contends there was a discrepancy in the testimony of Ms. KB because she testified that she tried to find Grievant in the afternoon of April 10, 2003 but her reply email was sent at 10:49 a.m. Grievant did not specify what significance he believes should be attached to that supposed discrepancy. If he is attempting to question the credibility of Ms. KB, the Hearing Officer found her testimony to be credible. Indeed, when Ms. KB returned to work several days later she brought Grievant a gift. There is little reason to believe that Ms. KB's testimony was adversely affected by animosity towards Grievant.

Grievant contends there are six witnesses but the Hearing Officer's ruling only shows five witnesses. The hearing decision lists the appearance of individuals. Since the Agency Party Designee, Mr. GP, was already listed as appearing at the hearing, it was unnecessary to list him a second time as a witness.

Grievant contends that the testimony of the Agency's Security Director and Grievant Exhibits 4 and 5 show that Grievant demonstrated his full support of the Agency's data security policies and practices. It is not clear that the exhibits and testimony support Grievant's contention. Nevertheless, Grievant's actions to assist

those outside of Zenworks may have reflected Grievant's helpfulness, but he was not asked or expected to provide such assistance.

Grievance hearings are normally limited to one day. Grievant spent a substantial portion of his presentation cross examining Agency witnesses regarding points not in dispute. Grievant admitted making changes to various objects. It was unnecessary to cross examine Agency witnesses regarding the mechanics of his making those changes. On several occasions, the Hearing Officer cautioned Grievant regarding his use of time but Grievant continued focusing on insignificant points in the Agency's case rather than focusing on his defense in chief. If Grievant had made better use of his time, more of his witnesses could have been heard.

Grievant's request for reconsideration does not identify any newly discovered evidence or any incorrect legal conclusions. Grievant simply restates the arguments and evidence presented at the hearing. For this reason, Grievant's request for reconsideration is **denied.**

APPEAL RIGHTS

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

1. The 10 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. The agency shall request and receive prior approval of the Director before filing a notice of appeal.

_____

Carl Wilson Schmidt, Esq.
Hearing Officer

POLICY RULING OF THE DEPARTMENT OF
HUMAN RESOURCE MANAGEMENT

In the matter of
The Department of Motor Vehicles
February 11, 2004

The grievant has requested an administrative review of the hearing officer's September 26, 2003, decision in Case No. 5801. The grievant objects to the hearing officer's decision because he believes that the Group III Written Notice that was issued was not consistent with the violation and does not fall within the human resource management guidelines. He also states that there are many untruths and misrepresented facts cited in the ruling. The grievant also requested that the hearing officer reconsider his decision. The agency head, Ms. Sara Redding Wilson, has requested that I respond to this administrative review request.

FACTS

The Department of Motor Vehicles (DMV) employed the grievant as a Computer Systems Senior Engineer before he was terminated. On June 3, 2003, the grievant was issued a Group III Written Notice with termination and the charges were as follows:

> Safe, reliable, and secure computer Network Systems are essential to the effective operations of the Agency. Employee was computer systems senior engineer. He formerly worked in LAN/Network Security and after certain rights were removed by Network Security, system records show he knowingly and intentionally reinstated those rights and gave certain access those rights to others, thereby violating the security practices and protocol in which he had been trained and certified. This resulted in undermining the agency's IT communication activities and programs.

The grievant filed a grievance and the hearing officer upheld management officials' disciplinary actions. In his reconsideration decision, the hearing officer did not modify his position.

The grievant formerly held a position that gave him security access to agency employees' accounts to provide technical assistance to those employees when needed. In providing this technical assistance he remotely could control employees' computers to assist them in resolving problems. When he was transferred to another position within the agency, management officials removed those access rights. Without management officials' permission, he reestablished those access rights as well as the access rights of others. Thus, management officials deemed that this action represented a serious breach in security that warranted a Group III Written Notice with removal.

The relevant policy, the Department of Human Resource Management's Policy No.1.60, Standards of Conduct, states that it is the Commonwealth's objective to promote the well being of its employees in the workplace and to maintain high standards of professional conduct and work

performance. This policy also sets forth (1) standards for professional conduct, (2) behavior that is unacceptable, and (3) corrective actions that agencies may impose to address behavior and
employment problems. Section V, Unacceptable Standards of Conduct, of that policy sets forth, but is not all-inclusive, examples of unacceptable behavior for which specific disciplinary action may be warranted.

In summary, in the instant case the Grievant was charged with taking action that created a very serious breach of the Network Security system. For that violation, DMV felt that it was of such a serious nature that it warranted termination.

DISCUSSION

Hearing officers are authorized to make findings of fact as to the material issues in the case and to determine the grievance based on the evidence. In addition, in cases involving discipline, the hearing officer reviews the facts to determine whether the cited actions constitute misconduct and whether there are mitigating circumstances to justify reduction or removal of the disciplinary action. If misconduct is found but the hearing officer determines that the disciplinary action is too severe, he may reduce the discipline. By statute, this Department has the authority to determine whether the hearing officer's decision is consistent with policy as promulgated by DHRM or the agency in which the grievance is filed. The challenge must cite a particular mandate or provision in policy. This Department's authority, however, is limited to directing the hearing officer to revise the decision to conform to the specific provision or mandate in policy. This Department has no authority to rule on the merits of a case or to review the hearing officer's assessment of the evidence unless that assessment results in a decision that is in violation of policy and procedure.

In the present case, the hearing officer determined that there was sufficient evidence to support the allegations the agency made against the grievant. DHRM Policy No. 1.60, Standards of Conduct, provides guidance to agencies for handling workplace misconduct and behavior and for taking corrective action. The issues you raised in your challenge are evidentiary rather than policy related. Please be reminded that it is not the role of this Agency to review the evidence unless the assessment by the hearing officer results in a decision that is contrary to policy. This Agency has determined that the hearing officer's decision comports with the provisions of Policy No. 1.60 and will not interfere with the decision.

If you have any questions regarding this correspondence, please call me at (804) 225-2136.

Sincerely,

Ernest G. Spratley
Manager, Employment
Equity Services