



# COMMONWEALTH OF VIRGINIA

*Department Of Human Resource Management*

*Office of Employment Dispute Resolution*

## DECISION OF HEARING OFFICER

In re:

**Case number: 11997**

**Hearing Date: October 3, 2023**

**Decision Issued: November 21, 2023**

### PROCEDURAL HISTORY

On June 12, 2023, Grievant was issued a Group II written notice for disciplinary action with termination for unsatisfactory performance and failure to follow instructions or policy for leaving his username and password written down and unattended inside a drawer in the staff office.

On June 12, 2023, Grievant was issued a Group II written notice for disciplinary action with termination for unsatisfactory performance and failure to follow instructions or policy for allowing multiple residents to access the staff office and allowing residents to be left alone inside the staff office on October 2, 2022, October 29, 2022, and November 20, 2022.

On June 12, 2023, Grievant was issued a Group III written notice for disciplinary action with termination for unsatisfactory performance, failure to follow instructions or policy and unauthorized use of state property or records for utilizing unauthorized software to access prohibited internet content, including music and pornographic images on October 2, 2022, October 29, 2022, and November 20, 2022.

On July 11, 2023, Grievant timely filed a grievance to challenge the Agency's action. The matter advanced to hearing. On August 7, 2023, the Office of Employment Dispute Resolution assigned this appeal to the Hearing Officer. On October 3, 2023, a hearing was held at Agency offices at the Facility.

*An Equal Opportunity Employer*

## **APPEARANCES**

Grievant  
Grievant's Advocate  
Agency Representative  
Agency Party Designee  
Witnesses

## **ISSUES**

1. Whether Grievant engaged in the behavior described in the Written Notices?
2. Whether the behavior constituted misconduct?
3. Whether the Agency's discipline was consistent with law (e.g., free of unlawful discrimination) and policy (e.g. properly characterized as a Group I, II or III offense)?
4. Whether there were mitigating circumstances justifying a reduction or removal of the disciplinary action, and if so, whether aggravating circumstances existed that would overcome the mitigating circumstances?

## **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. The employee has the burden of raising and establishing any affirmative defenses to discipline and any evidence of mitigating circumstances related to discipline. 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 Juvenile Justice employed Grievant as a Security Officer IV – Resident Specialist I at one of its facilities until his removal on June 12, 2023. No evidence of prior active disciplinary action was introduced during the hearing.

Grievant was normally assigned to the Unit in the Facility and had access to the Staff Office in the Unit which housed an Agency computer (the Unit Computer).

On October 2, 2022, Grievant was working at the Facility from approximately 5:50 AM until approximately 10:15 PM, with a break from 3:00 PM until 4:00 PM.<sup>1</sup> The logbook page for the Unit for October 2, 2022 indicates that Grievant reported to the Unit at 5:45

---

<sup>1</sup> Agency Ex. at 46.

AM to relieve staff and begin his shift on the Unit with Employee W. Grievant made entries in the logbook throughout the day on October 2, 2022 and was relieved of duty on the Unit at approximately 6:15 PM.

On or about November 23, 2022, the Virginia Information Technology Agency (VITA) notified the Agency that it was investigating suspicious activity that originated from the Unit Computer under a user account for which VITA identified Grievant as the account holder.

At all times relevant to this case, Grievant was the account holder for the user account identified by VITA as generating suspicious activity on the Unit Computer.

VITA determined that unauthorized software known as "Psiphon" had been downloaded onto the Unit Computer. "Psiphon" is an open-source internet software that is used to bypass and circumvent virtual private networks and proxy security measures. Psiphon allows users to bypass security measures and access internet sites that would normally be blocked.

Following the notification from VITA, the Unit Computer was seized and the system secured so that VITA could conduct a more thorough investigation of the suspicious activity that had occurred utilizing the Unit Computer.

The Agency also opened an internal investigation into the matter.

Because the Agency received the notification from VITA on November 23, 2022, Agency personnel initially thought that the suspicious activity had occurred on that date. However, the investigation revealed that suspicious activity had not occurred on November 23, 2022, but had occurred on other dates.

As part of its investigation, VITA accessed the master file table on the Unit Computer which is a record of any file that is created or accessed on a specific computer system. The master file table includes time stamps for creation, modification, and access to each specific file. VITA also identified "link files" on the Unit Computer. For each file that is accessed on a computer, there is a "link file" that is created that identifies where it ran, who ran it, and what time it ran.

VITA's investigation revealed that Grievant's user account was utilized to download Psiphon and to access music and sexually explicit pornographic material on the Unit Computer at various times, including on October 2, 2022, October 29, 2022, and November 20, 2022.

As part of the Agency's internal investigation, Special Agent also reviewed Rapid Eye video footage from the Unit for the dates and times initially identified by VITA, including October 2, 2022, October 29, 2022, and November 20, 2022. The Agency's Rapid Eye system writes over video footage after certain varying lengths of time. Special Agent saved onto his Agency-issued computer, video footage from the Unit's Rapid Eye system based on the dates and times initially identified by VITA as when suspicious activity occurred on the Unit Computer. At some point after the investigation, Special Agent's computer crashed and only some of the video footage was retrievable from Special

Agent's hard drive and available for the hearing in this matter. Some video footage from October 2, 2022, was available for the hearing. Video footage from October 29, 2022, and November 20, 2022 was not available for the hearing.

As part of the internal investigation, the Employee Relations Consultant was provided special permission to access the sites identified by VITA that were accessed by Grievant's computer user account. The Employee Relations Consultant confirmed those sites contained sexually explicit content.

## **CONCLUSIONS OF POLICY**

Unacceptable behavior is divided into three types of offenses, according to their severity. Group I offenses "include acts of minor misconduct that require formal disciplinary action."<sup>2</sup> Group II offenses "include acts of misconduct of a more serious and/or repeat nature that require formal disciplinary action." Group III offenses "include acts of misconduct of such a severe nature that a first occurrence normally should warrant termination."

### **Group II Written Notice – Leaving Username and Password Written Down and Unattended**

The Department of Juvenile Justice has issued Administrative Procedure #VOL I-1.3-3 regarding Information Security IDs and Passwords. The stated purpose of the procedure is "[t]o ensure users of the Department of Juvenile Justice's (DJJ) network and the Virginia Juvenile Justice Information System (VJJIS) access the network and VJJIS in accordance with Virginia state laws, regulations, and the Virginia Information Technologies Agency's requirements, policies, and standards."<sup>3</sup> The procedure requires that the Department of Juvenile Justice's (DJJ's) Information Technology Services (ITS) "shall assign unique IDs and passwords to each user for DJJ's computers and other specialized applications" and that "[p]asswords shall not be revealed to anyone under any circumstances, without exception."<sup>4</sup> "Users are not permitted to allow another person to log on to any computer using their account information (ID/Password) .... Users are accountable for any activity on the system performed with the use of their account. There is no exception [ ] to this rule."<sup>5</sup>

The procedure makes clear that "[a]ny violation of these policies and procedures shall be treated as a security violation with appropriate action being taken. ... [f]or classified

---

<sup>2</sup> The Department of Human Resources Management ("DHRM") has issued its Policies and Procedures Manual setting forth Standards of Conduct for State employees.

<sup>3</sup> Agency Ex. at 115, Department of Juvenile Justice, Information Technology Services Administrative Procedure, Administrative Procedure # VOL I-1.3-3, Subject: Information Security IDs and Passwords § I.

<sup>4</sup> Agency Ex. at 116, Department of Juvenile Justice, Information Technology Services Administrative Procedure, Administrative Procedure # VOL I-1.3-3, Subject: Information Security IDs and Passwords § V.C.2.

<sup>5</sup> Agency Ex. at 116, Department of Juvenile Justice, Information Technology Services Administrative Procedure, Administrative Procedure # VOL I-1.3-3, Subject: Information Security IDs and Passwords § V.C.3.

employees, the various levels of the Commonwealth's Standards of Conduct may be used, including termination."<sup>6</sup>

Whether Grievant engaged in the behavior described in the Written Notice and whether the behavior constituted misconduct

Special Agent testified that when he interviewed Grievant and asked if Grievant had shared his login information with anyone, Grievant stated that he left his username and password written down and unattended inside a drawer in the Staff Office on the Unit and that he did so due to a work injury that made it difficult for Grievant to remember his login information.

Grievant testified that during the Agency's investigation he told Special Agent that because he had trouble remembering his password to access the Agency's computer network, on some occasions, he would write his password on a piece of paper which he would put in a drawer in the desk in the Staff Office on the Unit where it was easily accessible to him. Grievant testified that he only did this while he was "on the Unit" on those occasions when he forgot a notebook that he normally kept in his pocket for notes. Grievant testified that he "did not leave it overnight." Grievant testified that the Staff Office door was always locked, such that, on those occasions when he left his password on a piece of paper in the desk drawer, it was accessible only to other Agency staff with keys to the Staff Office. Grievant also testified that on some occasions when he did not have his notebook, he believed he might have put a piece of paper with his password on it into his pocket which he believed could have inadvertently fallen out of his pocket without his knowledge.

Grievant testified that he knew that writing down his password and leaving it unattended was a violation of policy.<sup>7</sup>

Grievant argued that his trouble remembering his password is the result of a concussion that he suffered as a work-related injury that occurred on March 3, 2022.<sup>8</sup> Following the injury, Grievant was released to return to work full time full duty on June 22, 2022.<sup>9</sup> There do not appear to have been any restrictions on Grievant's return to work. Grievant admitted that he did not inform the Agency that he had trouble remembering his password and he did not ask the Agency for an accommodation. According to Grievant he did not ask for an accommodation because "they wouldn't do that because it's against the policy."<sup>10</sup> There is not enough information in the record to determine whether Grievant's past injuries and trouble remembering his password would qualify as a disability under the Americans with Disabilities Act. Such analysis is not necessary in this case, however, because, although the Americans with Disabilities Act requires employers to provide reasonable accommodations for an employee's disability, it does not broadly shield employees from disciplinary action for their own misconduct, especially in a situation such

---

<sup>6</sup> Agency Ex. at 115-116, Department of Juvenile Justice, Information Technology Services Administrative Procedure, Administrative Procedure # VOL I-1.3-3, Subject: Information Security IDs and Passwords § V.B.

<sup>7</sup> Hearing recording at 2:40:32-2:40:38.

<sup>8</sup> Agency Ex. at 80.

<sup>9</sup> Agency Ex. at 81.

<sup>10</sup> Hearing recording at 2:40:09-2:40:32.

as this where the Agency was unaware of Grievant's trouble remembering his password and Grievant did not ask for an accommodation because he did not believe the Agency would allow him to write down his password because to do so would violate policy.

Grievant violated policy that prohibited him from revealing his password to others when he wrote down his password and placed it in a drawer in the Staff Office that he knew was accessible to individuals other than himself.

Whether the Agency's discipline was consistent with law and policy

Violation of policy is a Group II offense. An Agency may suspend an employee without pay for up to 10 days for a Group II offense. A Group II offense may result in termination only if there are other active written notices such that the accumulation of offenses warrants termination.

The Agency's termination of Grievant's employment for this Group II offense is consistent with policy if Grievant has another active Group II (or Group III) offense.

**Group II Written Notice – Allowing residents to access the Staff Office**

The Department of Juvenile Justice has a Standard Operating Procedure for the movement and supervision of residents that requires staff supervising residents to

always position themselves where they will have maximum sight supervision. Whenever residents are in their rooms or other unit areas, staff shall be positioned for optimum viewing of resident activities. Staff shall minimize the use of the unit office. The unit office shall be used only for official business.<sup>11</sup>

The Facility's Security Post Order for Resident Specialist I directs that

[t]he unit staff office is to be locked at all times. A resident will not be allowed to enter the staff office for any reason. Violation of this policy will result in discipline according to the Standards of Conduct.<sup>12</sup>

Whether Grievant engaged in the behavior described in the Written Notices and whether the behavior constituted misconduct

The Agency asserts that Grievant allowed residents to access the Staff Office on October 2, 2022, October 29, 2022 and November 20, 2022. Special Agent testified that when reviewing Rapid Eye video footage from the Unit consistent with the dates and times that Grievant's user account was used to access unauthorized content, Special Agent observed footage showing what appeared to be Grievant allowing residents to access the Staff Office. Special Agent's notes reflect his observations of Grievant's and residents' movements in relation to the Staff Office from the video footage from October 2, 2022,

---

<sup>11</sup> Agency Ex. at 135, Department of Juvenile Justice, Division of Residential Services, Standard Operating Procedure, VOL IV-4.1-2.04, Subject: Movement and Supervision of Residents § 2.04-4.1, 9.

<sup>12</sup> Agency Ex. at 49-74.

October 29, 2022 and November 20, 2022. At some point after the investigation, Special Agent's computer crashed and only video footage from October 2, 2022 was available for the hearing in this matter. Video footage from October 29, 2022 and November 20, 2022 was not available for the hearing and was not available in advance of the hearing for Grievant's review.

Special Agent testified that when he interviewed Grievant during the investigation Grievant indicated that he would both stream and download music on the Unit Computer because he liked to play music for the residents while he was working on the Unit. Special Agent testified that he asked Grievant specifically about Rapid Eye video from October 2, 2022 which appeared to show that Grievant was on duty on the Unit, allowed residents into the Staff Office and then at one point exited the Staff Office while residents were in the Staff Office alone. Special Agent testified that Grievant told him he may have left the residents in the Staff Office listening to music while he went out onto the floor to check on other residents.

Grievant testified that he did not allow any residents to access the Staff Office and that residents showed him respect by standing in the doorway of the Staff Office and not entering the Staff Office when Grievant was in the Staff Office. Grievant testified that when he was questioned during the investigation, he told Special Agent that he did not allow residents into the Staff Office and may have said that he left residents standing in the doorway of the Staff Office when he exited the Staff Office.<sup>13</sup>

The only video footage available during the hearing was dated October 2, 2022 from approximately 1:11:13 PM to 1:29:11 PM (Video 1) and from 1:51:18 PM to 2:18:04 PM (Video 2). The footage shows the Unit "day room" which is a large open area on the Unit. The video footage is from two cameras capturing two different angles of the day room for the same time period. One camera (View 1) is situated along one wall of the Staff Office facing the day room. The other camera is situated on an opposite wall (View 2) and shows as its far view the wall of the Staff Office including a window that appears to look into the Staff Office. Neither camera is situated to provide a direct view of the door to the Staff Office. According to the Unit diagram, the door to the Staff Office is situated slightly around the corner from the area shown in the video footage along a short "hallway."<sup>14</sup> The short hallway that runs alongside the Staff Office is not viewable from the video footage. That hallway leads to a locked door that provides access to the shower area which includes a toilet area. Beyond the door to the shower area is another locked door that provides access to a locked cleaning supply closet.

Employee W, who also was working on the Unit on October 2, 2022, appears in the video footage identified as Video 1 (1:11:13 PM to 1:29:11 PM), but does not appear in the video footage identified as Video 2 (1:51:18 PM to 2:18:04 PM). The Agency was not able to specifically determine Employee W's location during that time, but suggested that Employee W may have been on a break or otherwise away from the Unit during that time.<sup>15</sup>

---

<sup>13</sup> Hearing recording at 2:47:17-2:50:07.

<sup>14</sup> Agency Ex. at 79. According to Special Agent, the door to the Staff Office is identified at "208" on the Unit diagram.

<sup>15</sup> Employee W is no longer employed with the Agency, was not interviewed as part of the investigation into this matter, and did not testify during the hearing.

Video footage identified as Video 1 (1:11:13 PM to 1:29:11 PM) shows Grievant and Employee W working on the Unit. During the video, at various points, Grievant disappears around the corner toward the Staff Office door. At varying times during the video, individual residents disappear around the corner toward the Staff Office door and reappear immediately or within a minute or two. Video 1 does appear to show one resident that disappears around the corner toward the Staff Office door and does not reappear for approximately 10 minutes. At one point during this period, Employee W also disappears around the corner toward the Staff Office door. In Video 2, a resident disappears around the corner toward the Staff Office door for at least 20 minutes during which time Grievant reappears from having disappeared around the corner toward the Staff Office door (the footage ends before the resident returns into view of the camera). Employee W never appears on the Video 2 footage and, although the Unit logbook suggests that Employee W was still on post on the Unit, it is unclear where Employee W is during this time.

Grievant argued that the video footage from October 2, 2022 shows residents leaving the day room and disappearing around the corner near the Staff Office door. Grievant suggests that there are other reasons those residents could have disappeared around the corner without entering the Staff Office. Grievant suggests that the residents may be standing in the doorway of the Staff Office, using the toilet in the shower room, going to a supply closet to gather cleaning supplies or cleaning the shower room.<sup>16</sup>

Based on the limited views of the video footage available for October 2, 2022 and without a better understanding of the size of the short hallway where the Staff Office door is located, the Hearing Officer cannot conclude that the Agency has met its burden of proof that Grievant allowed residents to access the Staff Office.

#### Whether the Agency's discipline was consistent with law and policy

Because the Agency has not met its burden of proving that the Grievant engaged in misconduct, the Agency's discipline was not consistent with policy.

Because the Agency has not met its burden of proof, there is no need to consider mitigating or aggravating factors with respect to the discipline issued pursuant to this Group II Written Notice.

#### **Group III Written Notice – Utilizing prohibited software to access prohibited content on the Unit Computer**

The Agency's Information Resource Acceptable Use procedure sets forth

a prescriptive set of processes and procedures, aligned with applicable Commonwealth of Virginia (COV) Information Technology (IT) security policy and standards, to ensure the Department of Juvenile Justice develops, disseminates, and updates the Information Resource Acceptable Use Administrative Procedure

---

<sup>16</sup> Hearing recording at 2:19:06-2:19:27; 2:20:32-2:22:38.

requirements as stipulated by the COV Information Technology Resource Management (ITRM) Security Standard SEC501 and security best practices. This procedure explains responsibilities for use of DJJ information technology resources (including but not limited to computer systems, mobile devices, voicemail, electronic mail (email), Local Area Network LAN, and Internet connection on DJJ devices), specifies the actions that are prohibited, and establishes the minimum requirements for the Information Resource Acceptable Use Procedure.<sup>17</sup>

The Information Resource Acceptable Use procedure “applies to all DJJ IT users to whom a COV network account has been assigned, as well as all DJJ systems (including but not limited to computers, mobile devices, electronic mail, etc.).”<sup>18</sup>

The Information Resource Acceptable Use procedure provides

DJJ IT Users shall not use any access control mechanism<sup>19</sup> that has not been expressly assigned to them and shall not disclose or modify any assigned or entrusted access control mechanism for any purpose other than those required to perform any authorized employment functions unless properly authorized to do so in writing by the Director or the Information Security Officer (ISO).<sup>20</sup>

The Information Resource Acceptable Use procedure makes clear that “DJJ personnel shall only use software that is part of the IT standard software suite or that has been approved by the IT Director” and that “[s]treaming media (music or movie streaming) unless its use is business related” is prohibited.<sup>21</sup>

The Information Resource Acceptable Use procedure also provides that

[i]n addition to unacceptable uses as defined in DHRM’s Policy 1.75, Use of Electronic Communications and Social Media, the following statements, although not inclusive, define specific unacceptable uses for DJJ’s network and systems. DJJ personnel shall not:

...

b. Access download, print, or store sexually explicit material in violation of § 2.2-2827 of the Code of Virginia.

...

---

<sup>17</sup> Agency Ex. at 118, Department of Juvenile Justice, Administrative Procedure, Administrative Procedure # VOL I-1.3-7, Subject: Information Resource Acceptable Use § I.

<sup>18</sup> Agency Ex. at 118, Department of Juvenile Justice, Administrative Procedure, Administrative Procedure # VOL I-1.3-7, Subject: Information Resource Acceptable Use § II.

<sup>19</sup> Access control mechanism is defined in this Administrative Procedure as “any login identifiers, passwords, terminal identifiers, user identifiers, digital certificates, IP addresses, logon IDs granted to the DJJ IT Users.” Agency Ex. at 119.

<sup>20</sup> Agency Ex. at 121, Department of Juvenile Justice, Administrative Procedure, Administrative Procedure # VOL I-1.3-7, Subject: Information Resource Acceptable Use § IV.B.1.

<sup>21</sup> Agency Ex. at 121, Department of Juvenile Justice, Administrative Procedure, Administrative Procedure # VOL I-1.3-7, Subject: Information Resource Acceptable Use § C.

f. Tamper with or otherwise attempt to circumvent security controls e.g. hardware, software, image, operating system integrity standards, and anti-virus software.

...

p. Download, install, or distribute, without the authorization of the Director, ISO, or designee:

- i. Games.
- ii. Screen Savers programs.
- iii. Peer-to-peer file-sharing programs.
- iv. Non-VITA supported software.<sup>22</sup>

Further, Virginia law prohibits state employees from utilizing “agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content.”<sup>23</sup>

#### Whether Grievant engaged in the behavior described in the Written Notices and whether the behavior constituted misconduct

Grievant’s computer user account was used to download the Psiphon software onto the Unit Computer without specific authorization in violation of the Information Resource Acceptable Use Procedure.

Grievant’s computer user account was used to access sexually explicit content on the Unit Computer in violation of the Information Acceptable Use Procedure and Virginia law.

Grievant admits to streaming music on the Unit Computer but denies accessing sexually explicit content on the Unit Computer (or any Agency computer). Because Grievant sometimes worked on other units, Grievant argues that the Agency is speculating when it asserts that Grievant was working on the Unit and had access to the Unit Computer on the dates and times when the Psiphon software was downloaded and executed and when sexually explicit content was accessed.

Although Grievant testified that sometimes he would work on other units, he also testified that he normally worked on the Unit. The Agency provided timesheets showing that Grievant was working at the Facility on the dates and times when Grievant’s computer user account was used to access the Psiphon software and the prohibited content.<sup>24</sup> The Agency provided the Unit log for October 2, 2022 which shows Grievant starting his post on the Unit at approximately 5:45 AM and being relieved from his post on the Unit at approximately 6:15 PM. The Agency also provided Rapid Eye video footage from cameras on the Unit dated October 2, 2022 from approximately 1:11:13 PM to 1:29:11 PM and from 1:51:18 PM to 2:18:04 PM which shows Grievant working on the Unit and

---

<sup>22</sup> Agency Ex. at 123-125, Department of Juvenile Justice, Administrative Procedure, Administrative Procedure # VOL I-1.3-7, Subject: Information Resource Acceptable Use § F.

<sup>23</sup> Va. Code § 2.2-2827. "Sexually explicit content" means (i) any description of or (ii) any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting sexual bestiality, a lewd exhibition of nudity, as nudity is defined in § 18.2-390, sexual excitement, sexual conduct or sadomasochistic abuse, as also defined in § 18.2-390, coprophilia, urophilia, or fetishism.

<sup>24</sup> Agency Ex. at 46-48.

with access to the Unit Computer. Information from VITA's investigation of the Unit Computer shows that the unauthorized software and sexually explicit content was accessed on the Unit Computer using Grievant's user account on October 2, 2022<sup>25</sup> while Grievant was working on the Unit with access to the Unit Computer.<sup>26</sup> Special Agent testified that the data VITA pulled from the Unit Computer has time stamps in Greenwich Mean Time whereas the Rapid Eye video footage and the Unit log book would reflect local time.<sup>27</sup>

The VITA investigation revealed that Grievant's user account also was used to access prohibited content on October 29, 2022 and November 20, 2022. Time sheets show that Grievant was working at the Facility on October 29, 2022 and November 20, 2022 during the times VITA identified suspicious activity associated with Grievant's user account.<sup>28</sup> The video footage showing Grievant working on the Unit on October 29, 2022 and November 20, 2022 was not available for the hearing. Special Agent credibly testified that his computer crashed at some point following the investigation into this matter and that the video footage from October 2, 2022 was the only footage retrievable from his computer's hard drive. The Agency was able to provide the Special Agent's report which included the Special Agent's observations from his review of video footage from the Unit. Special Agent's report includes Special Agent's observation from the video footage that Grievant was working on the Unit with access to the Unit Computer on October 29, 2022 and November 20, 2022.<sup>29</sup>

The Agency has met its burden of proving that Grievant utilized unauthorized software and accessed prohibited internet content, including sexually explicit material on the Unit Computer. The Hearing Officer finds that even considering only the allegations and evidence related to October 2, 2022, the Agency has met its burden of proof.<sup>30</sup>

#### Whether the Agency's discipline was consistent with law and policy

Failure to comply with policy or misuse of state property typically is a Group II offense. In this case, the Agency has presented sufficient evidence to support elevation of the offense to a Group III offense because of the serious nature of the offense and because Grievant's actions also constituted a violation of § 2.2-2827(B) of the Code of Virginia which prohibits an agency employee from accessing sexually explicit content. Additionally, Grievant's actions accessing unauthorized software designed to circumvent the Commonwealth's information security measures present a security breach to the Agency's information technology systems.

Upon the issuance of a Group III Written Notice, an agency may remove an employee.

---

<sup>25</sup> Agency Ex. at 23-38 and 39-43.

<sup>26</sup> Agency Ex. 46-48 and 142.

<sup>27</sup> Because the Hearing Officer was unsure whether the Rapid Eye video footage from October 2, 2022 is set to Eastern Standard Time or Daylight Savings Time, she considered the evidence under both scenarios.

<sup>28</sup> Agency Ex. at 47-48.

<sup>29</sup> Agency Ex. at 32-35.

<sup>30</sup> Because the Hearing Officer was unsure whether the Rapid Eye video footage from October 2, 2022 is set to Eastern Standard Time or Daylight Savings Time, she considered whether the Agency had met its burden under both scenarios and was satisfied that it had.

## Mitigation

Virginia Code § 2.2-3005.1 authorizes hearing officers to order appropriate remedies including “mitigation or reduction of the agency disciplinary action.” Mitigation must be “in accordance with rules established by the Department of Human Resource Management...”<sup>31</sup> Under the Rules for Conducting Grievance Hearings, “[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. If the hearing officer mitigates the agency’s discipline, the hearing officer shall state in the hearing decision the basis for mitigation.” A non-exclusive list of examples includes whether (1) the employee received adequate notice of the existence of the rule that the employee is accused of violating, (2) the agency has consistently applied disciplinary action among similarly situated employees, and (3) the disciplinary action was free of improper motive. In light of this standard, the Hearing Officer finds no mitigating circumstances exist to reduce the disciplinary action.

## DECISION

For the reasons stated herein, the Agency’s issuance to Grievant of a Group II written notice for disciplinary action with termination for unsatisfactory performance and failure to follow instructions or policy for leaving his username and password written down and unattended inside a drawer in the staff office with termination is **upheld**.

For the reasons state herein, the Agency’s issuance to Grievant of a Group II written notice for disciplinary action with termination for unsatisfactory performance and failure to follow instructions or policy for allowing multiple residents to access the staff office and allowing residents to be left alone inside the staff office is **rescinded**.

For the reasons stated herein, the Agency’s issuance to Grievant of a Group III written notice for disciplinary action with termination for unsatisfactory performance, failure to follow instructions or policy and unauthorized use of state property or records for utilizing unauthorized software to access prohibited internet content, including music and pornographic images is **upheld**.

## APPEAL RIGHTS

You may request an administrative review by EDR within **15 calendar** days from the date the decision was issued. Your request must be in writing and must be **received** by EDR within 15 calendar days of the date the decision was issued.

<sup>32</sup>

Please address your request to:

Office of Employment Dispute Resolution

---

<sup>31</sup> Va.Code § 2.2-3005.

Department of Human Resource Management  
101 North 14<sup>th</sup> St., 12<sup>th</sup> Floor  
Richmond, VA 23219

or, send by e-mail to [EDR@dhrm.virginia.gov](mailto:EDR@dhrm.virginia.gov), or by fax to (804) 786-1606.

You must also provide a copy of your appeal to the other party and the hearing officer. The hearing officer's **decision becomes final** when the 15-calendar day period has expired, or when requests for administrative review have been decided.

A challenge that the hearing decision is inconsistent with state or agency policy must refer to a particular mandate in state or agency policy with which the hearing decision is not in compliance. A challenge that the hearing decision is not in compliance with the grievance procedure, or a request to present newly discovered evidence, must refer to a specific requirement of the grievance procedure with which the hearing decision is not in compliance.

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.<sup>33</sup>

  
\_\_\_\_\_  
Angela L. Jenkins, Esq.  
Hearing Officer

---

<sup>33</sup> 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.