COMMONWEALTH OF PENNSYLVANIA

William Hutnick	:	State Civil Service Commission
	:	
v.	:	
	:	
Pennsylvania Emergency Management Agency	:	Appeal No. 31134

William Hutnick	Megan Madaffari
Pro Se	Attorney for Appointing Authority

ADJUDICATION

This is an appeal by William Hutnick challenging his Level-Two Alternative Discipline in Lieu of Suspension[1] from regular Clerical Assistant 2 employment with the Pennsylvania Emergency Management Agency. A hearing was held on November 2, 2023, via video, before Commissioner Gregory M. Lane.

The Commissioners have reviewed the Notes of Testimony and exhibits introduced at the hearing. The issue before the Commission is whether there is good cause for appellant's Level-Two ADLS.

[1] Under the ADLS, there was no effect on appellant's pay, seniority, or other benefits. The Level-Two ADLS carries the same weight as if appellant served a three-day suspension. Comm. Ex. A. Consequently, the present appeal will be considered by the Commission as an appeal of a three-day suspension.

FINDINGS OF FACT

1. By letter dated June 15, 2023, appellant was issued a Level-Two Alternative Discipline in Lieu of Suspension (hereinafter "ADLS") with final warning equivalent to a three-day suspension, from regular Clerical Assistant 2 employment with the Pennsylvania Emergency Management Agency. Comm. Ex. A.

2. The June 15, 2023, Level-Two ADLS letter provides the following:

> The reason for this action is your 1) Unauthorized use of Department tools and/or equipment, and 2) Violation of the Commonwealth internet usage policy. Specifically, you used your Department issued computer and Commonwealth internet account to view non-business-related websites, including inappropriate sexual/pornographic sites, during your normal working hours for non-business related purposes.

Comm. Ex. A.

3. The appeal was properly raised before this Commission and was heard under Section 3003(7)(i) of Act 71 of 2018. Comm. Ex. C.

4. Appellant is employed as a Clerical Assistant 2 and is responsible for engaging in mailroom operations and receiving mail. N.T. p. 85; AA Ex. 13.

5. Appellant's duties as a Clerical Assistant 2 do not require him to browse on the internet during his work hours. N.T. pp. 86-87; AA Exs. 13, 14.

6. On July 15, 2021, appellant signed, acknowledged, and agreed to abide by the Commonwealth's Internet Use Policy, Management Directive 205.34 (hereinafter "Management Directive"). N.T. pp. 83-84; AA Ex. 12.

7. The Management Directive outlines the Acceptable Use Standards for Commonwealth employees, including appellant, to operate Commonwealth issued devices and Information Technology (hereinafter "IT") resources. N.T. pp. 71-72; AA Ex. 10.

8. The Management Directive lists unacceptable uses of IT resources, including but not limited to, accessing, or viewing material in any medium considered to be inappropriate or personally

offensive, such as sexually suggestive, pornographic, or obscene material. N.T. pp. 78-79; AA Ex. 10 (p. 17).

9. The Management Directive prohibits the use of non-standardized open-source software and downloading, distributing, and/or installing any unapproved software. N.T. pp. 77, 80; AA Ex. 10 (pp. 9, 18).

10. The Management Directive prohibits employees from participating in internet activities that inhibit an employee's job performance or present a negative image to the public, such as participating in auctions or playing games. N.T. p. 79; AA Ex. 10 (p. 17).

11. IT Policy Associate 2 Nicole Kennedy received compliance reports indicating appellant accessed pornographic and adult websites depicting sexually explicit content. N.T. p. 27.

12. Kennedy submitted the compliance reports to Human Resources. N.T. p. 27.

13. Kennedy received a request from Human Resources to investigate and review appellant's internet activity for the fall of 2022 and spring of 2023. N.T. p. 26.

14. The investigation resulted in the creation of appellant's Full Detail Log reflecting the types of websites he accessed and viewed from February 2023 to May 2023. N.T. p. 30; AA Ex. 1.

15. The Full Detail Log identified appellant based upon his username, "WHUTNICK" and source IP number. N.T. p. 31; AA Ex. 1.

16. Based on the Full Detail Log, Kennedy created a User Summary listing the total amount of unauthorized websites appellant accessed. N.T. p. 37; AA Ex. 2.

17. Appellant requested to access and viewed pornographic websites 494 times, websites containing adult material eighty-seven times, malicious websites 238 times, game websites forty-nine times, and websites categorized as "illegal or unethical" five times. N.T. pp. 37-38; AA Exs. 1, 2.

18. Appellant visited the following pornographic websites most frequently: 1) ancensored.com; 2) aznude.com; 3) coedcherry.com; 4) VIPactors.com; 5) wikiporno.com; and 6) ZBporn.com. N.T. pp. 44-46; AA Exs. 1, 2, 4.

19. During the course of the investigation, screenshots were taken of the pornographic websites appellant most frequently visited. These screenshots were sexually explicit by depicting naked men and women and illustrating oral and vaginal intercourse. AA Ex. 5.

20. During the investigation, the Office of Information Security assigned IT Executive 1 Kirk Mallein to conduct a forensic investigation on appellant's Department issued computer. N.T. pp. 57-58.

21. While there was no pornographic material downloaded onto the computer, Mallein's forensic investigation revealed appellant downloaded a private-based browser called "Opera." N.T. pp. 58-59.

22. The "Opera" browser erases all user activity once the browser is closed. N.T. pp. 58-59.

23. Appellant did not receive special permissions to download the "Opera" browser or any privacy-based web browser. N.T. p. 60.

DISCUSSION

The issue before the Commission in the present appeal is whether the appointing authority established good cause for appellant's Level-Two Alternative Discipline in Lieu of Suspension (hereinafter "ADLS"). Specifically, the appointing authority charged appellant with unauthorized use of his Department issued computer and violations against the Commonwealth's internet usage policy. Comm. Ex. A.

In an appeal challenging the suspension of a regular status employee, the appointing authority bears the burden of establishing good cause for the personnel action. *White v. Commonwealth, Department of Corrections*, 110 Pa. Commw. 496, 532 A.2d 950 (1986); 71 Pa.C.S.A. §§ 2603(c), 3003 (7)(i). Good cause must be based upon meritorious criteria and be related to one's competency and ability to execute job duties properly. *White*, 110 Pa. Commw. At 498, 532 A.2d at 951.

In support of its case-in-chief, the appointing authority presented the testimony of Information Technology (hereinafter "IT") Policy Associate 2 Nicole Kennedy,[2] IT Executive 1 Kirk Mallein,[3] and Human Resource Analyst 4 Anthony Reda.[4] Appellant elected not to present testimony or submit exhibits in response.

IT Policy Associate 2 Kennedy examines Commonwealth employee internet activity through reviewing weekly compliance reports.[5] N.T. pp. 21-22. The compliance reports reflect Commonwealth employees who have viewed adult content and violated the Commonwealth's Acceptable Use Standards. N.T. p. 22. Once she receives these reports, Kennedy verifies the reported activity. N.T. pp. 23-24. If the activity is verified, Kennedy submits her investigative findings to Human Resources. N.T. p. 24.

Kennedy testified she began observing appellant's name appear on compliance reports during September 2022 and May 2023.[6] N.T. p. 25. Specifically, the compliance reports reflected appellant accessed pornographic and adult type websites that depicted explicit sexual content. N.T. p. 27. Kennedy sent the

[2] Kennedy is employed by the appointing authority as an IT Policy Associate 2 and has held the position for over eight years. N.T. p. 19. Kennedy's responsibilities include conducting internet investigations and compliance reporting, facilitating policy updates, and creating new security policies. N.T. p. 21.

[3] Mallein is employed by the Office of Information Security as an IT Executive 1. N.T. p. 52. Mallein's responsibilities include conducting forensic investigations and assisting incident responses. N.T. p. 56.

[4] Reda is employed by the Office of Administration, Executive Offices, as a Human Resource Analyst 4. N.T. p. 64. Reda investigates violations against the Commonwealth's Management Directives. N.T. p. 71.

[5] Kennedy receives compliance reports once a week from the appointing authority's networking vendor. N.T. pp. 23-24.

[6] Kennedy recalled appellant appeared nearly two dozen times. N.T. p. 25. Kennedy has never seen an employee appear so many times on a compliance report in the eight years of being an IT Policy Associate. N.T. p. 26.

compliance reports to Human Resources. N.T. p. 25. Kennedy explained since appellant's conduct appeared so frequently and the reports indicated he viewed pornographic websites numerous times; she followed up with Human Resources. N.T. pp. 26, 28. As a result, Kennedy received a request from Human Resources to investigate and review appellant's internet activity for the fall of 2022 and spring of 2023. N.T. p. 26.

Kennedy's investigation resulted in the creation of appellant's Full Detailed Log. N.T. p. 30; AA Ex. 1. A Full Detailed Log shows the websites an employee visited during a set period of time. The Full Detailed Log records the username and user source IP with each website visited. The Full Detailed Log also categorizes the websites an employee has accessed. N.T. p. 30. The Full Detailed Log validates the source IP information and the data exchange between an employee's device and the accessed website. N.T. p. 30.

Kennedy explained if the user is permitted access, the user's action status will be shown as "allowed." N.T. p. 31. However, if a user attempts to access a website that contains material that is categorically prohibited by the Commonwealth's Internet Use Policy, *i.e.*, Management Directive 205.34, then the user's request will be denied, and their action status will be blocked. N.T. p. 35; AA Ex. 15. For example, an employee's request to access the website called "VIPactors.com" will be denied. N.T. p. 35; AA Ex. 15.

Kennedy described how appellant's action status was "allowed" when he accessed websites categorized as pornographic. N.T. p. 32; AA Ex. 1 (p. 12). Kennedy explained the appointing authority's firewall policies were not updated, which caused users to be allowed access to prohibited websites. The appointing

authority did not update their firewall policies until October 9, 2023. N.T. pp. 33-34; AA Ex. 15. As a result, appellant's firewall policies were not updated which improperly permitted him access to view pornographic websites between February 2023 through May 2023. N.T. pp. 34; AA Exs. 1, 2, 3, 4.

Based upon her review of appellant's Full Detailed Log, Kennedy created a User Summary outlining the websites appellant accessed. N.T. p. 37; AA Ex. 2. Appellant's User Summary reflects the number of requests to access categorized websites and the amount of data exchanged for each category. N.T. p. 37. Appellant's User Summary revealed appellant requested to access pornographic websites 494 times, websites containing adult material eighty-seven times, malicious websites 238 times, game websites forty-nine times, and websites categorized as "illegal or unethical" five times.[7] N.T. pp. 37-38, 41-42; AA Ex. 2. Kennedy confirmed appellant accessed and viewed these websites listed on the Full Detailed Log because appellant's username known as "WHUTNICK", and source IP number correctly identified him. N.T. p. 31; AA Ex. 1.

Additionally, Kennedy filtered from the Full Detailed Log each time appellant accessed pornographic websites and created a report reflecting appellant's activity. N.T. p. 38-39; AA Ex. 3. Kennedy discovered appellant began viewing pornographic websites on February 7, 2023, and continued viewing these types of websites until May 1, 2023. N.T. pp. 39-40; AA Ex. 3. Kennedy further observed

[7] Prior to the commencement of the hearing on October 18, 2023, the appointing authority and appellant stipulated and agreed to the nature of the appointing authority exhibits showing screenshots of pornographic websites listed on appellant's Full Detail Log. N.T. p. 50; AA Ex. 5. The complete description and details of these screenshots may be found in AA Ex. 5.

appellant accessed pornographic websites during work hours. Specifically, the Full Detailed Log data reflected appellant accessed pornographic websites between 7:00 a.m. and 3:30 p.m. N.T. pp. 42-43; AA Exs. 1, 3; *see Finding of Fact 18.* Kennedy confirmed appellant accessed these pornographic websites because appellant's username, "WHUTNICK" was recorded in the Full Detail Log. N.T. p. 39-40; AA Exs. 1, 3.

Meanwhile, after Kennedy's compliance reports were submitted to Human Resources, Human Resources contacted the Office of Information Security to conduct a forensic investigation on appellant's Department issued computer. N.T. p. 57. IT Executive 1 Mallein was assigned to appellant's investigation. He used a forensic program called EnCase Forensics to conduct and pull a bit-by-bit forensic read-only copy of appellant's computer's hard drive. N.T. p. 57. Mallein compared the read-only copy of appellant's hard drive with the internet reports to review what occurred on appellant's computer. N.T. p. 58.

Based upon his review, Mallein did not find any downloaded pornography on appellant's computer. N.T. p. 58. However, Mallein discovered appellant installed a browser called "Opera" that is not a standard browser or approved by the Commonwealth.[8] Specifically, "Opera" is a privacy-based web browser that allows the user to hide his activity by default. "Opera" runs in the computer's memory space. As a result, "Opera" erases the user's activity once the browser is closed. N.T. pp. 58-59. Mallein could not review how appellant used

[8] Mallein confirmed users are prohibited from installing unauthorized private-based browsers. N.T. p. 59.

"Opera" or where appellant visited online using "Opera." N.T. pp. 60-61. Mallein confirmed through the investigation that appellant did not receive special permission to download "Opera" or any privacy-based web browser. N.T. p. 60. Yet, Mallein was able to confirm appellant used "Opera" because the browser would launch auto-updates when opened. N.T. pp. 62-63. Although appellant used "Opera," Mallein noted appellant used Google Chrome and a Microsoft browser on his computer. N.T. p. 60.

During the investigation, the Office of Administration's Office of Investigations sent Human Resource Analyst 4 Reda the list of websites appellant visited. N.T. p. 67. Whenever Reda receives a list of prohibited websites an employee allegedly accessed, Reda attempts to view the accessed content. Reda could not access the websites appellant visited because he was blocked. N.T. p. 67. Nevertheless, Reda was able to review the investigation's screenshots of the websites listed on appellant's Full Detail Log that were categorized as pornographic and confirmed they were pornographic and sexually explicit in nature. N.T. p. 68.

Reda further reviewed appellant's training transcript. N.T. p. 81. Reda confirmed appellant received annual training regarding Security Awareness and Acceptable Use since 2013. N.T. p. 81; AA Ex. 11. Appellant's Security Awareness and Acceptable Use training includes training about the Management Directive. N.T. p. 82. On July 15, 2021, appellant signed the Employee Conduct Expectations agreeing and acknowledging to abide by the Commonwealth's Management Directive 205.34 (hereinafter "Management Directive"). N.T. pp. 83-84; AA Ex. 12.

All Commonwealth employees are required to review and acknowledge their receipt of the Management Directive. N.T. p. 70; AA Ex. 10. It provides the Acceptable Use Standards for Commonwealth employees to operate Commonwealth issued devices and IT resources.[9] N.T. pp. 71-72; AA Ex. 10. The Management Directive lists improper and unauthorized uses of IT resources or Commonwealth data by authorized users that could result in disciplinary action, up to and including termination of employment. AA Ex. 10 (p. 3).

Specifically, the Management Directive states, "authorized [u]sers may not use IT Resources or any unauthorized assets/devices to leverage IT Resources to access, create, store, transmit, post, or view material that is generally considered to be inappropriate or personally offensive or which may be construed as discriminatory or harassing, including sexually suggestive, pornographic, or obscene material." AA Ex. 10 (p. 9). Additionally, it provides "[a]uthorized [u]sers may not use non-standardized open-source software, shareware, or freeware software (i.e., unauthorized resources) without OA/OIT prior approval generated through established policy exception processes." N.T. p. 77; AA Ex. 10 (p. 9). This prohibition includes "downloading, distributing, and/or installing any unapproved software." N.T. p. 80; AA Ex. 10 (p. 18).

Notably, the Management Directive lists unacceptable uses of IT resources. All authorized users are prohibited from the following:

> Accessing, creating, storing, transmitting, posting, or viewing material in any medium that is generally considered to be inappropriate or personally offensive or which may be construed as harassing or threatening

[9] IT resources are tools that the Commonwealth has made available for Commonwealth business purposes. AA Ex. 10 (p. 5).

> activities, including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, offensive material, sexually suggestive, pornographic, or obscene material.

N.T. pp. 78-79; AA Ex. 10 (p. 17). The Management Directive further prohibits employees from participating in Internet activities that inhibit an employee's job performance or present a negative image to the public, such as participating in auctions or playing games. N.T. p. 79; AA Ex. 10 (p. 17).

Upon review of appellant's Full Detail Log, Reda considered appellant's use of IT resources as unreasonable. Reda described how appellant used his authorized access to shop on the internet, access travel and gaming websites, and visit prohibited websites, including pornography. N.T. pp. 75-76. Reda also contended appellant's installation of the "Opera" browser would constitute unauthorized software. N.T. p. 77.

Reda supported his consideration by reviewing appellant's position description as a Clerical Assistant 2. Appellant's responsibilities include engaging in mailroom operations and receiving mail. Appellant's work hours are from 8:00 a.m. to 4:00 p.m. N.T. p. 85; AA Ex. 13. Reda testified none of appellant's duties require him to browse the internet during work hours. N.T. pp. 86-87; AA Exs. 13, 14.

After Reda reviewed the investigation's findings, he contacted the appointing authority to schedule appellant a pre-disciplinary conference. N.T. pp. 67-68. Reda testified based upon the investigation's findings and his review of the Management Directive, appellant's discipline was warranted. Reda explained

appellant's discipline was appropriate because appellant used his Commonwealth issued computer for unauthorized uses in violation of the Management Directive. N.T. p. 91.

Appellant elected not to provide any testimony or submit any exhibits on the record in response to the appointing authority's case-in-chief. Instead, appellant argued during his closing statement the appointing authority failed to establish wrongdoings of his personal computer station regarding supposed browsing on banned websites except to arcane references to Internet spam or adware. N.T. pp. 99. Appellant argued Reda contacted the AFSCME union which resulted in a union representative contacting him to persuade his to accept the discipline. N.T. pp. 99-100. Appellant also asserted the appointing authority did not establish the charges because no pornographic material was found on his device or hard drive. N.T. p. 100. Similarly, appellant contended he did not violate the Management Directive because Reda could not access the listed websites to determine if they were offensive. N.T. pp. 100-101. Lastly, appellant argued Reda's review of the printed screenshots of the listed websites and their thumbnails allowing malicious codes into server drives. N.T. pp. 101-102.

Having carefully reviewed the record, as a whole, the Commission finds the appointing authority established good cause to issue appellant's Level-Two ADLS. We find the testimonies of Nicole Kennedy, Kirk Mallein, and Anthony Reda credible[10] and persuasive regarding appellant's unauthorized online activity in violation of the Commonwealth's Management Directive outlining the Acceptable Use Standards. The uncontested evidence revealed appellant used his Department

[10] It is within the purview of the Commission to determine the credibility of the witnesses. *State Correctional Institution at Graterford, Department of Corrections v. Jordan*, 95 Pa. Commw. 475, 478, 505 A.2d 339, 341 (1986).

issued computer to not only visit prohibited websites, including but not limited to pornographic and sexually explicit material, but also installed a prohibited private-based software concealing his activities when the program deleted them from the device. These actions negatively impact appellant's competency and ability to perform his responsibilities and duties as a Clerical Assistant 2 by directly violating the instructions set forth in the Management Directive, as stated above.

Regarding appellant's arguments during his closing statement, we find them unpersuasive attempts to excuse and invalidate his misconduct. First, there is no evidence of record regarding the interactions between Reda and appellant's union regarding his discipline. In fact, there is no testimony on record reflecting any AFSCME involvement. Moreover, the Commission only granted appellant's appeal under § 3003 (7)(i) of Act 71 of 2018. Therefore, no claims of discrimination were permitted to be heard in this appeal.

Furthermore, while appellant's device did not have downloaded pornographic material within his device or hard drive, Kennedy, Mallein, and Reda provided ample credible explanations and details on how appellant used his Department issued computer in unauthorized and prohibited ways, including but not limited to installing a private-based web browser, accessing gaming websites, and viewing pornographic and sexually explicit content during work hours. The Commission also notes Reda credibly explained he was unable to access the listed websites appellant viewed because he was blocked due to their potentially violative nature.

Lastly, the Commission finds appellant's assertion of Reda allowing malicious codes into the server drives and violating the Management Directive when he printed screenshots of the listed websites and thumbnails to be preposterous. The stipulated screenshots were printed pursuant to an investigation into whether appellant used Commonwealth resources to access unauthorized and prohibited websites. When the screenshots were printed, Reda was acting in conformance with his responsibilities and duties in conducting the investigation. Appellant's attempt to evade scrutiny for his blatant misuse of Commonwealth resources will simply not stand. Accordingly, we find appellant's Level-Two ADLS warranted and enter the following:

CONCLUSIONS OF LAW

The appointing authority has presented evidence establishing good cause for suspension under Section 2603 of Act 71 of 2018.

ORDER

AND NOW, the State Civil Service Commission, by agreement of its members, dismisses the appeal of William Hutnick challenging his Level-Two Alternative Discipline in Lieu of a three-day suspension from regular Clerical Assistant 2 employment with the Pennsylvania Emergency Management Agency

and sustains the action of the Pennsylvania Emergency Management Agency in the Level-Two Alternative Discipline in Lieu of a three-day suspension of William Hutnick from regular Clerical Assistant 2 employment.

State Civil Service Commission

Maria P. Donatucci
Chairwoman

Gregory M. Lane
Commissioner

Pamela M. Iovino
Commissioner

Issued: February 27, 2024