COMMONWEALTH OF PENNSYLVANIA

Ryan L. Bowersox	:	State Civil Service Commission
	:	
v.	:	
	:	
Office of Administration,	:	
Executive Offices	:	Appeal No. 30549

Ryan L. Bowersox	Jonathan W. Kunkel
Pro Se	Attorney for Appointing Authority

ADJUDICATION

This is an appeal by Ryan L. Bowersox challenging his removal from regular Network Administrator 1 employment with the Office of Administration, Executive Offices. A video hearing was held on November 24, 2020, via Skype for Business, before Commissioner Bryan R. Lentz.

The Commissioners have reviewed the Notes of Testimony and exhibits introduced at the hearing. The issue before the Commission is whether the appointing authority had just cause for appellant's removal.

FINDINGS OF FACT

1. On April 13, 2020, appellant was informed he was removed from his regular Network Administrator 1 employment with the appointing authority, effective April 14, 2020. Comm. Ex. A; AA Ex. 12.

2. The April 13, 2020 removal letter provides the following reason for appellant's removal:

> **Violation of Management Directive 245.18**: Specifically, on February 5, 2020, you used your IT Administrator privileges to access a contracted employee's files remotely without her permission and where no business-related reason existed.
>
> **Violation of Management Directive 205.34**: Specifically, during a forensic review of your commonwealth issued computer in March 2020, it was discovered that you stored multiple photographs of a woman who is frontally nude to a personal cell phone that was backed up to your commonwealth issued computer.

Comm. Ex. A (emphasis in original).

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

4. On February 10, 2020, HR Analyst 2 Emily Shapard received a complaint alleging appellant used his IT administrator privileges as a Network Administrator 1 to access a contracted employee's Commonwealth issued computer files remotely. N.T. p. 31.

5. After reviewing the complaint, Shapard and her supervisor, Chief of Employee Relations for the General Government Human Resource Delivery Center Matthew Updegrove, conducted an investigation into appellant's misconduct. N.T. pp. 31, 33, 113.

6. Updegrove and Shapard interviewed appellant and the contracted employee. N.T. pp. 31, 33.

7. On February 11, 2020, appellant was suspended pending investigation.[1] N.T. pp. 32, 36.

[1] Appellant did not appeal his suspension pending investigation. Comm. Ex. C.

8. Updegrove and Shapard requested an email capture for appellant's and the contracted employee's Microsoft Outlook history to review whether there were any communications related to the complaint's allegations. The email capture did not find any communications between appellant and the contracted employee. N.T. pp. 36-37.

9. After the email capture was reviewed, IT Administrator 1 Kirk Mallein conducted a forensic capture of appellant's and the contracted employee's Commonwealth issued computers. N.T. p. 70.

10. Based on the forensic capture of appellant's Commonwealth issued computer, Mallein discovered appellant used his IT administrator privileges to open, view, and close the contracted employee's picture, Notepad document, OneNote document, and desktop file remotely on February 5, 2020. N.T. pp. 85-88; AA Ex. 5.

11. The forensic capture did not identify any indication the contracted employee remotely accessed appellant's Commonwealth issued computer. N.T. p. 106.

12. While conducting the forensic capture of appellant's and the contracted employee's Commonwealth issued computers, Mallein performed default forensic searches for human faces and nude photography. N.T. p. 71.

13. During the default forensic searches for human faces and nude photography, Mallein found appellant uploaded and stored ten frontally nude photographs of a woman onto his Commonwealth issued computer. N.T. pp. 96-97; AA Ex. 7.

14. Based on Mallein's submitted final report, Shapard and Mallein concluded appellant remotely accessed the contracted employee's Commonwealth issued computer without her permission. N.T. pp. 39-40.

15. On April 7, 2020, appellant received a pre-disciplinary conference via a Skype conference call. N.T. pp. 40, 42; AA Ex. 1.

DISCUSSION

This issue in the present appeal is whether the appointing authority established just cause for appellant's removal from regular Network Administrator 1 employment. Specifically, the appointing authority charged appellant with violating two Management Directives. First, the appointing authority charged appellant with violating Management Directive 245.18 on February 5, 2020, by using his IT administrator privileges to access a contracted employee's Commonwealth issued computer files remotely without her permission and without a business-related reason. Comm. Ex. A; AA Ex. 12. Second, the appointing authority charged appellant with violating Management Directive 205. 34 because during a forensic review of his Commonwealth issued computer in March 2020, it was discovered appellant stored multiple photographs of a woman who is frontally nude to his personal cell phone that was backed up onto his Commonwealth issued computer. Comm. Ex. A; AA Ex. 12. Either charge, standing alone, would warrant appellant's removal. Comm. Ex. A; AA Ex. 12.

The appointing authority bears the burden of proving just cause for removal of a regular status employee and must prove the substance of the charges underlying the removal. *Long. v. Commonwealth of Pennsylvania Liquor Control Board,* 112 Pa. Commw. 572, 535 A.2d 1233 (Pa. Commw. 1988). Factors supporting the just cause removal of a civil service employee must be related to the employee's job performance and touch in some logical manner upon the employee's competency and ability to perform his job duties. *Woods v. State Civil Service Commission,* 590 Pa. Commw. 337, 912 A.2d 803 (2006).

In support of its charges, the appointing authority presented the testimony of HR Analyst 2 Emily Shapard,[2] IT Administrator 1 Kirk Mallein,[3] and Chief of Employee Relations for the General Government Human Resource Delivery Center Matthew Updegrove.[4] In response, appellant testified on his own behalf.

Shapard received a complaint against appellant on February 10, 2020. The complaint alleged appellant used his IT administrator privileges to remotely access a contracted employee's Commonwealth issued computer. N.T. p. 31. After receiving and reviewing the complaint, Shapard and Updegrove conducted an investigation into the allegation against appellant. N.T. pp. 31, 33. Updegrove worked alongside Shapard, as her supervisor, throughout appellant's disciplinary investigation. N.T. p. 113. Shapard and Updegrove began the investigation by interviewing appellant and the contracted employee. N.T. pp. 31, 33. During appellant's interview, Shapard showed appellant the complaint. N.T. p. 35. In response, appellant denied the allegation that he used his IT administrator privileges to remotely access the contracted employee's Commonwealth issued computer. Instead, Shapard explained appellant alleged the contracted employee remotely accessed his Commonwealth issued computer and her own Commonwealth issued computer to set him up. N.T. pp. 34-35.

---

[2] Emily Shapard is employed as an HR Analyst 2 for the General Government Human Resource Delivery Center at the Office of Administration. N.T. p. 26. As a HR Analyst 2, Shapard investigates allegations of employee misconduct and recommends disciplinary action to the appointing authority. N.T. p. 29.

[3] Kirk Mallein is employed as an IT Administrator 1. N.T. p. 64. As an IT Administrator 1, Mallein's duties include conducting investigations, forensic captures, incident responses, and reverse engineering. N.T. p. 65.

[4] As the Chief of Employee Relations for the General Government Human Resource Delivery Center, Updegrove is responsible for overseeing the Employee Relations Program for sixteen agencies, including the appointing authority, under the Office of Administration's Office of Information Technology. N.T. p. 112.

Following the interviews, Shapard testified appellant was suspended pending investigation on February 11, 2020. N.T. pp. 32, 36. Shortly thereafter, Shapard and Updegrove requested an email capture for appellant's and the contracted employee's Microsoft Outlook history. N.T. p. 36. An email capture is a screenshot of an employee's Microsoft Outlook history, including sent messages and Skype history. N.T. p. 36. Once the email capture was complete, Shapard reviewed the email capture. During the review, Shapard searched for any communications between the contracted employee and appellant. N.T. p. 37. Shapard testified she did not find anything from the email capture relating to the complaint against appellant. N.T. pp. 38, 55. After the email capture was reviewed, Shapard presented the results of the email capture to the Office of Administration's Executive Management. Shapard testified it was determined a forensic capture of appellant's and the contracted employee's Commonwealth issued computers be conducted. N.T. p. 38.

Pursuant to the determination, Mallein conducted a forensic capture of appellant's and the contracted employee's Commonwealth issued computers. N.T. p. 70. A forensic capture is a bit-by-bit copy of a computer that an analyst can observe by using forensic software. N.T. p. 70. Pursuant to the forensic capture, Mallein looked for appellant's and the contracted employee's names, Commonwealth issued computers, and IP addresses. N.T. p. 70. Afterwards, Mallein requested appellant's and the contracted employee's Commonwealth issued computers in order to connect them to the forensics machine to conduct the forensic capture. N.T. p. 70. Once Mallein completed the forensic capture, he opened the Magnet Forensic software program. Mallein imported the forensic capture's copies

of appellant's and the contracted employee's Commonwealth issued computer's hard drive contents to the Magnet Forensics software program. N.T. p. 71. Through the Magnet Forensics software program, Mallein reviewed the imported contents with a focus on what transpired on February 5, 2020. N.T. p. 72. During the review, Mallein performed default forensic searches on both Commonwealth issued computers for drugs, violence, hate speech, human faces, and nude photography. N.T. p. 71. Based on his review of appellant's computer, Mallein created Forensic Examination Reports addressing his discoveries.[5] N.T. pp. 73, 89; AA Exs. 5, 7.

Mallein provided an explanation of the first Forensic Examination Report's construction and details. Mallein explained the keywords used to conduct the forensic search were the appellant's and the contracted employee's names and usernames. N.T. pp. 75-76; AA Ex. 5. Once he entered the keywords, Mallein collected a list of twenty records. Within each record, there are the following subjects: tags, display name, content, activity type, date, source and location. AA Ex. 5. First, Mallein explained the tags within each record identify the type of information discovered during the search. Mallein labeled each tag as "Evidence." N.T. pp. 76-77; AA Exs. 5, 7. Second, the display name within the record was the actual name of the file used as evidence. Third, the content listed within the record is the exact location of the file that was discovered. N.T. p. 77; AA Ex. 5. Mallein emphasized the character "c$" within the content's section of the record signifies a user used his IT administrator privileges to access the computer's file remotely. N.T. pp. 77-78; AA Ex. 5. A normal user would be unable to connect and view the content

[5] The Forensic Examination Report lists the machine's name, manufacturer, serial number, and hard drive size. N.T. p. 74; AA Ex. 5.

without IT administrator privileges. N.T. p. 81. Fourth, the activity type within each record described what the user did when he accessed the file. N.T. p. 82. Fifth, the dates and times within each record show the times a user performs an activity. N.T. p. 82. Sixth, the source within each record identifies the user who accessed the contents. N.T. p. 83; AA Ex. 5.

According to the forensic capture of appellant's Commonwealth issued computer, Mallein testified appellant used his IT administrator privileges, to remotely access the contracted employee's picture, Notepad document, OneNote document, and desktop file. N.T. pp. 85-86, 87-88; AA Ex. 5. As presented by the record's content section, Mallein noted appellant used his administrator privileges due to the "c$" being recorded. N.T. p. 85; AA Ex. 5.[6] Additionally, the record's content section presents the contracted employee's username, "c-ashankar," as the owner of the accessed contents. AA Ex. 5. Mallein explained appellant was the user accessing the contract employee's contents because appellant's username, "rybowersox," was identified within each record's source. AA Ex. 5. Mallein noted appellant opened, viewed, and closed the contracted employee's Commonwealth issued computer's contents multiple times in succession from 7:38 AM to 7:49 AM. N.T. pp. 82-83, 88; AA Ex. 5. Mallein testified the forensic search of the contracted employee's Commonwealth issued computer did not identify any indication the contracted employee accessed appellant's Commonwealth issued computer. N.T. p. 106.

[6] Mallein confirmed the contracted employee possessed similar administrator privileges as appellant. N.T. p. 104.

While performing the forensic search and review, Mallein discovered appellant possessed ten frontally nude photographs of a woman on his Commonwealth issued computer. N.T. p. 96; AA Ex. 7.[7] Within the second Forensic Examination Report, Mallein noted the date, source, and image size for each photograph being uploaded into appellant's Commonwealth issued computer. N.T. p. 97; AA Ex. 7. Mallein explained appellant's photographs were uploaded into his Commonwealth issued computer by plugging an iPhone into the device. Once plugged into the Commonwealth issued computer, the photographs were backed up into iTunes. N.T. p. 98. Mallein asserted an employee would have installed the iTunes program onto the Commonwealth issued computer by either receiving permission from their supervisor or by using IT administrator privileges. N.T. pp. 99-100. Mallein testified appellant would have had to install iTunes onto his Commonwealth issued computer to upload the photographs. N.T. p. 100. Mallein affirmed Commonwealth employees are not permitted to back up their personal photographs to their Commonwealth issued computers. N.T. p. 99. After the forensic search and review, Mallein submitted his final report. Upon reviewing the final report, Shapard and Mallein concluded appellant remotely accessed the contracted employee's Commonwealth issued computer without her permission. N.T. pp. 39-40. Updegrove reviewed all the information Shapard gathered pursuant to appellant's investigation. N.T. p. 113.

[7] The appointing authority and appellant agreed to stipulate that the discovered photographs were of a woman frontally nude. N.T. p. 94.

Following the forensic capture, appellant received a pre-disciplinary conference (hereinafter "PDC") via a Skype conference call on April 7, 2020. N.T. pp. 40, 42; AA Ex. 1. Updegrove conducted appellant's PDC along with Shapard. N.T. p. 114. During appellant's PDC, Updegrove and Shapard provided appellant an opportunity to explain his conduct in relation to the charges against him. N.T. p. 115. In response to the first charge of appellant using his IT administrator privileges to access the contracted employee's files remotely, Updegrove testified appellant denied the charge. Additionally, appellant asserted the contracted employee was out to ruin his life. N.T. p. 116. Updegrove confirmed appellant acknowledged an employee could only remotely access another employee's computer files with their permission. N.T. p. 116. In response to the second charge regarding appellant's possession of photographs of a woman frontally nude, Updegrove explained appellant asserted it was a mistake when the photographs were uploaded into his Commonwealth issued computer when he plugged in his personal iPhone. N.T. p. 117. During his PDC, appellant also confirmed he used his IT administrator privileges to install iTunes without his supervisor's permission. N.T. p. 117.

After his PDC, appellant was given forty-eight hours to provide any additional information that he would like the appointing authority to consider prior to making a disciplinary determination. N.T. p. 42. Shapard testified appellant submitted an email providing additional information on April 7, 2020. N.T. pp. 43, 118; AA Ex. 4. Updegrove reviewed appellant's additional information. N.T. pp. 118-119; AA Ex. 4. In his email, appellant described his thirteen years of service, his personal medical needs, and years of services as a Marine. Appellant did not present a rebuttal to the presented charges against him during his PDC. AA Ex. 4.

Updegrove described how appellant's misconduct violated Management Directive 245.18 and Management Directive 205.34. First, Management Directive 245.18 states Administrators "have the ability to create, access, modify and/or delete electronic resources, data and systems configurations within a given technology discipline as well as granting permissions to other individuals commensurate with their own privileges in a given technology discipline." N.T. p. 123; AA Ex. 2. Appellant was entrusted with rights and privileges that are greater than other users. Because of this, appellant was held to the "highest standards of professional and ethical conduct in the use of and administration of CoPA IT resources." N.T. pp. 123-124; AA Ex. 2. Pursuant to Management Directive 245.18, failure to protect the integrity or the security of the network or misuse of administrator authority is grounds for immediate discipline. N.T. p. 124; AA Ex. 2. Updegrove asserted appellant betrayed the Commonwealth's and appointing authority's trust when appellant used his IT administrator privileges to access the contracted employee's Commonwealth issued computer files remotely for his own personal gain. N.T. pp. 127-128. As such, Updegrove emphasized appellant failed to act in accordance with the highest standard of professional conduct as a Network Administrator 1. N.T. p. 127.

Second, Management Directive 205.34's objective is "to ensure all Authorized Users that have access to IT Resources are made aware of and comply with the standards and policy set forth in this directive and in Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources." N.T. pp. 119-120; AA Ex. 3. Within the attached Enclosure 1, it provides "Authorized Users may not 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." N.T. pp. 120-121; AA Ex. 3. Updegrove explained appellant violated Management Directive 205.34 by storing frontally nude photographs on his Commonwealth issued computer. N.T. p. 121.

Updegrove testified a decision was made to remove appellant from his Network Administrator 1 position. Comm. Ex. A; N.T. pp. 118-119; AA Ex, 12. On April 13, 2020, appellant received his removal letter. Comm. Ex. A; N.T. p. 45; AA Ex. 12. Shapard explained appellant's violations of Management Directive 245.18 and Management Directive 205.34 were the basis of his removal. Comm. Ex. A; N.T. pp. 47; AA Exs. 2, 3, 12.

In response to the appointing authority's presentation, appellant testified on his own behalf. Appellant testified he had a personal relationship with the contracted employee. As time progressed, appellant asserted their personal relationship began to fall apart in November 2019 after the contracted employee realized he was in a relationship with his partner. N.T. pp. 133-134. Appellant alleged the contracted employee wanted to get him back for talking to other coworkers about her in February 2020. N.T. pp. 137, 143. Appellant acknowledged receiving an email from the contracted employee asking him if he accessed her Commonwealth issued computer, which he denied. N.T. p. 137. Appellant denied accessing the contract employee's Commonwealth issued computer files remotely. N.T. pp. 143, 145.

Appellant argued the contracted employee accessed his Commonwealth issued computer instead. N.T. p. 143. Appellant stated the contracted employee had the same IT administrator privileges as him. N.T. pp. 138, 156. Appellant believed the contracted employee would have been able to

reprogram his computer to appear that he was accessing her Commonwealth issued computer remotely. N.T. p. 158. Appellant further alleged the contracted employee was able to access his Commonwealth issued computer because he was locked out of it due to his password being changed. N.T. p. 157. However, appellant admitted he did not have evidence to support his allegation that the contracted employee accessed his computer besides his testimony. N.T. pp. 150, 156.

Appellant also admitted to installing iTunes on his Commonwealth issued computer. Appellant stated his supervisor also installed iTunes and together, they both enjoyed listening to music when they worked. N.T. pp. 139-140. Appellant admitted plugging his iPhone into his Commonwealth issued computer. When the nude photographs were uploaded into his Commonwealth computer, appellant acknowledged "it was a mistake." N.T. p. 141.

Appellant further argued the forensic review of his Commonwealth issued computer was incomplete. Appellant stated the Commonwealth's domain controllers would be able to indicate when he logged into his Commonwealth issued computer and when he changed his password. N.T. pp. 156-157. Rebutting appellant's assertions regarding the Commonwealth's domain controllers, the appointing authority presented Mallein's explanation about how domain controllers could have impacted the forensic review of appellant's computer. Mallein explained the Commonwealth's domain controllers are not used to monitor when a user logs into or out of a Commonwealth issued computer. N.T. p. 168. Mallein testified having the domain controller's information would not have impacted the results of the forensic review of appellant's Commonwealth issued computer. N.T. p. 169.

Having carefully reviewed the record, the Commission finds the appointing authority presented just cause to establish appellant's removal. In support of our conclusion, we find credible the testimony of Emily Shapard, Kirk Mallein, and Matthew Updegrove.[8] The appointing authority presented two reasons supporting appellant's removal: 1) appellant violated Management Directive 245.18 by using his IT administrator privileges to remotely access a contracted employee's Commonwealth issued computer files without her permission and without a business-related reason; and 2) appellant transferred and stored multiple nude photographs on his Commonwealth issued computer from his iPhone.

The Commission will first address the issue of appellant's abuse of his IT administrator privileges. As a Network Administrator 1, and pursuant to Management Directive 245.18, appellant was responsible for adhering to the highest levels of professionalism and ethical conduct in the use of his IT administrator privileges because he was granted higher privileges than other Commonwealth users. Mallein credibly explained through the forensic capture of appellant's Commonwealth issued computer that appellant remotely accessed the contracted employee's picture, Notepad document, One Note document, and desktop file on her Commonwealth issued computer without her permission. Although appellant presents conclusory allegations that the contracted employee accessed his computer remotely instead, we find these allegations without merit. Moreover, Mallein credibly testified his forensic review of the contracted employee's Commonwealth

[8] 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,* 505 A.2d 339, 341 (Pa. Commw. Ct. 1986).

issued computer did not show the contracted employee remotely accessing appellant's Commonwealth issued computer. Despite appellant's assertion the forensic review was incomplete because the domain controllers were not reviewed, Mallein credibly presented how the domain controllers would not have affected the outcome of the investigation. As Updegrove credibly emphasized, appellant's clear misuse of his IT administrator privileges failed to protect the integrity of the network and betrayed the appointing authority's trust in granting him higher IT administrator privileges.

Having found appellant abused his IT administrator privileges, the Commission has determined that this charge standing alone warrants his removal. Therefore, we will not consider the merits of the second charge.[9] We find appellant's clear abuse of his IT administrator privileges is just cause for his removal as it negatively reflects upon his competency and ability to perform his job duties as a Network Administrator 1. *Woods*, *supra.* Accordingly, we enter the following:

[9] Appellant testified that he accidently uploaded the nude photographs into his Commonwealth issued computer by plugging in his iPhone. We note that Management Directive 240.11 provides that a connection of non-Commonwealth issued wireless communication device into a Commonwealth IT Resource, such as a Commonwealth issued computer, is considered a voluntary act for any authorized user. Management Directive 240.11 (5)(b)(1). Appellant voluntarily connected his iPhone to his Commonwealth issued computer and transferred and stored nude photographs on the computer. The connection and any improper business use, as defined in Management Directive 205.34, of non-Commonwealth issued devices may result in disciplinary action up to and including termination. Management Directive 240.11 (5)(b)(5).

CONCLUSION OF LAW

The appointing authority has presented evidence establishing just cause for removal under Section 2607 of Act 71 of 2018.

ORDER

AND NOW, the State Civil Service Commission, by agreement of its members, dismisses the appeal of Ryan L. Bowersox challenging his removal from regular Network Administrator 1 employment with the Office of Administration, Executive Offices, and sustains the action of the Office of Administration, Executive Offices in the removal of Ryan L. Bowersox from regular Network Administrator 1 employment, effective April 14, 2020.

State Civil Service Commission

Gregory M. Lane
Commissioner

Bryan R. Lentz
Commissioner

Mailed: March 22, 2021