1-13-2012

# CITY OF CHATTANOOGA, Petitioner, v. MARK TIMON, Grievant

**BEFORE THE ADMINISTRATIVE LAW JUDGE**
**ON BEHALF OF THE CITY COUNCIL OF THE CITY OF CHATTANOOGA**

| | | |
|---|---|---|
| **CITY OF CHATTANOOGA,** | ) | |
| **Petitioner,** | ) | |
| | ) | |
| **v.** | ) | **DOCKET NO. 56.00-114098J** |
| | ) | |
| **MARK TIMON,** | ) | |
| **Grievant.** | ) | |

**FINAL ORDER**

This contested case came on to be heard on January 13, 2012, in Chattanooga, Tennessee before Administrative Judge Joyce Grimes Safley, assigned by the Secretary of State, Administrative Procedures Division, and sitting for the City Council of the City of Chattanooga. Ms. Melinda Foster and Ms. Valerie Malueg, Assistant City Attorneys, represented the city of Chattanooga. The Grievant, Mr. Mark Timon, was present and was represented by Ms. Michelle Owens, attorney, of the Nashville Bar.

The transcript for this hearing was filed on January 23, 2012. The parties submitted their respective "Proposed Findings of Fact and Conclusions of Law" on January 24, 2012 and January 25, 2012, making this matter ripe for consideration.[1]

The subject of this hearing was Grievant's appeal of his termination from his employment as a Network Engineer with the City of Chattanooga.

T.C.A. §27-9-114, the City of Chattanooga's CIVIL SERVICE RULES (set forth in the CITY CODE), and RESOLUTION NO. 26612 OF THE CITY COUNCIL OF THE CITY OF CHATTANOOGA, govern this appeal.

---

[1] It is noted that the Final Order in this matter is due for issuance on or before twenty (20) days after the conclusion of the hearing. §11, RESOLUTION NO. 26612 OF THE CITY COUNCIL OF THE CITY OF CHATTANOOGA, ADMINISTRATIVE REGULATIONS FOR CONDUCT OF EMPLOYEE DISCIPLINARY HEARINGS. The hearing is deemed concluded and the record closed on the day of the last "filings" in this case. Accordingly, the Final Order is due on or before February 14, 2012.

Grievant was terminated for alleged: (1) inefficiency or negligence in the performance of his duties; and (2) violation of the City of Chattanooga Information Services' "Policy Governing Information Staff's Access to City of Chattanooga Data" (2000). Grievant argues there was not "cause" nor was there a "reasonable basis" for his termination because the alleged acts were not intentional; other employees who had *intentionally* given out the City of Chattanooga's computer system passwords to third parties were not terminated; no actual harm resulted to the City as a result of Grievant's mistake; and finally, Grievant argues that he did not receive due process prior to his termination.

After consideration of the testimony and evidence presented, the arguments of counsel, and the entire record in this matter, it is determined that the City of Chattanooga ("the City") proved, by a preponderance of the evidence, that Grievant mistakenly or negligently placed the City's computer system's "network passwords" into a "Dropbox" file[2] that he shared with Excalibur, a contractor with the City[3]. No actual harm to the City resulted from Grievant's mistake. The evidence preponderates that the decision to terminate Grievant was made prior to Petitioner's "*Loudermill* (due process) hearing". Accordingly, it is questionable whether Petitioner was afforded meaningful due process prior to being deprived of his employment. However, any lack

[2] "Dropbox" is a web-based file hosting service that uses "cloud storage" to enable users to store and share files and folders with others. "Cloud storage" is a term for a storage place or file where an individual can store information or data rather than placing such data on the individual's personal computer or any external devices such as a portable hard drive, thumb drive, flash drive, disk, etc.

[3] Grievant used the "Dropbox" file to share photographs needed for a work project with his project contact (Bobby Bullington) at Excalibur. Sharing the photographs with the Excalibur employee was necessary in order for them to work together on the project. However, Grievant did not realize that he had mistakenly "dragged" a "confidential file" (from his personal computer) containing Grievant's banking records, personal e-mail information, and and two current City "network passwords" into the "Dropbox".

of due process has been "cured" by this *de novo* hearing, such that Grievant's "due process" argument is **MOOT**. Finally, it is determined that there is not a "reasonable basis" or "just cause" to terminate Grievant's employment with the City.

The undersigned agrees with the City that Grievant made a very serious mistake, and discipline is appropriate. However, considering all the facts and circumstances of this matter, termination of Grievant is too harsh and is not "reasonable".

Accordingly, it is **ORDERED** that the appropriate discipline for Grievant's "mistake" or "negligence" is a ninety (90) day suspension without pay from September 23, 2011 until December 22, 2011.[4] Grievant shall be reinstated to his position as a Network Engineer with the City, and shall be made whole with regard to benefits, seniority, and lost wages (after the deduction of the 90 day suspension without pay).

## FINDINGS OF FACT

1. At the hearing of this matter, the City called the following as witnesses: (1) Mark Keil, (2) Jerod Windberry, (3) Le Ann Tinker, (4) Brent Page, (5) Chad Rowlee, (6) Bobby Bullington, (7) Chris Welch, and (8) Jana Lowery. Grievant's witnesses were: (1) Wes Floyd, (2) Mark Folsom, (3) Darryl Sheppard, and (4) Grievant Mark Timon. The City re-called Mark Keil as a rebuttal witness.

[4] It is noted that § 2-174 (c) of the CHATTANOOGA CITY CODE limits disciplinary suspensions of employees by the Mayor or a Department head to thirty (30) calendar days. However, no such restriction is placed upon the City Council or an Administrative Judge sitting for the City Council. Similarly, under State Civil Service Rules, while the appointing authority [the Department] may not suspend an employee without pay for greater than thirty days, the Civil Service Commission is not limited with regard to the actions it can take when it determines that dismissal of an employee is too harsh a disciplinary action. *See* T.C.A §8-30-325

*Background*

2. Grievant Mark Timon has been employed with the City of Chattanooga's Information Services ("IS") Department for almost eighteen (18) years.

3. The IS Department is responsible for the City's information system. Specifically, the IS Department manages the City's computer network technologies, supports its database and application servers, and manages its telephone network (including voice devices and applications).

4. Grievant began his employment with the City of Chattanooga as a computer programmer. He "wrote" the computer programs for many city departments. For a period of time, Grievant was the "webmaster" for the City of Chattanooga's internet website.

5. Grievant has an associate's degree in computer programming, and is a Cisco certified Network Assistant. In 2010, Grievant received his Cisco Certified Network Associate (CCNA) Security Specialization certificate.[5]

6. At that time, and continuing to the present time, he is the only IS Department employee who possesses all of these certifications.

7. Grievant held various positions within the IS Department over the years.

8. In 2004 Grievant received a three day suspension without pay for "below standard performance" based upon "slow work" and not completing work on time.

9. In 2005, Grievant received a one week suspension without pay for "unsatisfactory performance".

[5] Cisco Systems is a communications company which designs and sells electronics, networking, voice, and communications technology and services. The City of Chattanooga uses Cisco Systems for its communications system, which includes its computer network, voicemail, and other communication networks.

10. In 2006, Grievant was given a three day suspension without pay for completing assignments without following IS's Quality Assurance Policy.

11. Thereafter, Grievant's job performance improved and he was promoted to Network Engineer.

12. According to Chief Information Officer Mark Keil, the manager over the entire IS Department, Grievant's performance as a Network Engineer was "very good". CIO Keil also agreed that Grievant had always been "security conscious" regarding Information Services passwords during the past.

13. At least one witness described Grievant as the "go-to guy" with regard to his technical knowledge of networks and computers.

14. Network Manager Jerod Windberry, one of Grievant's supervisors, agreed that Grievant was a "good Network Engineer", and testified, credibly, that Grievant "knew his job" as a Network Engineer during the time Windberry supervised Grievant.[6]

15. The evidence preponderates that Grievant performed his job very well as a Network Engineer and was considered someone who was knowledgeable about his work.

16. After Grievant's 2006 "discipline", Grievant received no discipline or reprimands regarding his job performance until May, 2011 (after he had been promoted to the Security Analyst position.)

[6] Neither party offered any of Grievant's performance evaluations in evidence.

17. As a Network Engineer, Grievant was one of four people employed by the City of Chattanooga who were authorized to be in possession of the City's confidential "network passwords" which controlled the City's network.

18. Even Chief Information Officer Mark Keil, the department head for the Information Systems Department, was not one of the people authorized to possess the City's network passwords.

*Promotion to Security Analyst*

19. Grievant's job performance in the Network Engineer position was so good that in January 2011, Grievant was offered a promotion to "Security Analyst".

20. The Security Analyst position was a newly formed position in the Information Systems Department.

21. Grievant Timon was the first person to fill the Security Analyst position.

22. When Grievant was promoted to the "Security Analyst" position, he still had access to the City's "network passwords".

23. Network Manager Jerod Windberry testified that Grievant did not have access to the City's "network passwords" after his promotion to Security Analyst, and further testified that Grievant did not "need" the confidential "network passwords" in order to do his new job as Security Analyst.[7]

24. Network Manager Windberry described the newly created Security Analyst position held by Grievant as dealing with "physical securities, such as setting up cameras, doing evaluations on what would be needed,…access control to certain areas

[7]Jerod Windberry, Network Manager, directly supervised Grievant during the last few weeks of Grievant's time as a Security Analyst. Le Ann Tinker, Deputy Chief Information officer and Director of Technology, directly supervised Mr. Windberry.

throughout the City and being able to implement designs that would…help security on the security basis."

25. While Network Manager Windberry initially testified that Grievant did not need the City's confidential "network passwords" after his promotion to Security Analyst, Windberry later contradicted his earlier testimony and stated "He [Timon] knew them [the network passwords], and *we were shorthanded at the time,* and the fact that it was still a related…position, he was allowed to keep [the passwords]."[8]

26. Windberry's testimony also contradicts CIO Keil's testimony at the hearing. CIO Keil testified that after Grievant's promotion to Security Analyst, Grievant "should not have had access [to the passwords] at that point."

27. Neither Mr. Windberry's nor Mr. Keil's testimony is deemed credible regarding Grievant's supposed "lack of authority" to possess "network passwords" during Grievant's tenure as Security Analyst.

28. After Grievant was promoted to Security Analyst, he was not advised or instructed by IS management not to use the City's "network passwords".

29. Rather, the evidence preponderates that Grievant continued to assist with some Network Engineer duties and for that reason needed to possess and utilize "network passwords".

30. Grievant's new position as Security Analyst wasn't a "desk job". In addition to working on network security (firewalls, routers, switches), and the City surveillance camera systems, he was responsible for "NetMotion" (a mobile VPN private

[8] Windberry further testified that the "security analyst" position has been "back and forth" as far as whether fell within the "security side" or the "network side" of the Information Systems Department.

network client), the MESH system[9], going out into the field, doing security assessments on locations to see what was needed for physical security, and performing network assessment. Grievant was expected to meet with vendors (such as Excalibur), assess security needs at various locations, troubleshoot on location, and manage various security projects.

31. Grievant testified, credibly, that he often was required to work "in the field", including working in a "bucket truck" at 3:00 A.M. to make sure MESH was working at Riverbend; installing cameras on Saturday afternoons in city parking lots; going to vendor meetings; configuring routers and switches at various locations to connect back to the City's network, and evaluating new products for vendors.

32. Grievant further testified, convincingly, that in the new Security Analyst position, he had "more and more projects…coming down the pike faster than [he could] keep up with them."

33. Grievant had difficulty trying to keep up with his new projects and trying to keep up to date with his work.

34. This was compounded by the fact that in the Security Analyst position, Grievant also had deadlines for purchasing and using security equipment before various departments' "budget year" ended.

35. Clearly, Grievant was overwhelmed with the newly formed "Security Analyst" position, and was having difficulty keeping up with projects and deadlines. He made some mistakes.

[9] The MESH system is the City's wireless communication system.

36. Deputy Chief Information Officer/Technology Manager Le Ann Tinker testified, credibly, that Timon worked hard in his new position of Security Analyst, and "was attempting to do the work successfully."

37. During the hearing of this matter, several IS employees testified that Grievant "did a good job", was a "good worker", was a "good person", and was "trustworthy".

38. Various IS employees agreed that it was acceptable to share City information or "data" with vendors or contractors (such as Excalibur) when working together on projects.

39. In May, 2011, Grievant's supervisor, Deputy Chief Information Officer/ Director of Technology, Le Ann Tinker, "reprimanded" Grievant regarding some missed deadlines, and some complaints from certain City departments.

40. Grievant admitted to Ms. Tinker that he was having trouble in his new position as Security Analyst.

41. Sometime later in the summer, CIO Keil decided to have Technology Manager Windberry directly supervise Grievant, rather than Deputy CIO Tinker's being directly responsible for Grievant. Mr. Windberry began supervising Grievant in late June or July, 2011.

42. On August 11, 2011, Grievant was placed on "probation" by Network Manager Windberry.[10] On that date, Network Manager Windberry notified Grievant

[10] According to Network Manager Windberry's "30 day deadline", Grievant had until September 10, 2011 to improve his performance as Security Analyst prior to facing additional discipline. It is noted that the August 8, 2011 memorandum from Mr. Windberry to Grievant mistakenly stated that Grievant's "probationary period" was "extended". Actually, Grievant's six month "probationary period" in the new Security Analyst position had ended earlier in the summer.

that he had received complaints from some City department heads about the implementation and completion of certain projects; that there were complaints that Grievant was "reactive" rather than "proactive"; and that Grievant's work space had equipment sitting around and looked "unprofessional".[11] Mr. Windberry informed Grievant that he had thirty (30) days to improve his work performance or be subject to further disciplinary action.

43. Prior to the expiration of the thirty days "probation", according to CIO Keil, Grievant wrote a "very good and detailed letter…describing what he thought the problem was with his performance [as Security Analyst]."

44. In the letter or e-mail, Grievant stated that the problem was that he was "overworked". Grievant asked for a voluntary demotion back to his Network Engineer job. For unknown reasons, neither party entered the referenced e-mail into evidence at the hearing of this matter.

45. Grievant testified, credibly, that he wrote an e-mail to IS management specifically requesting a demotion, and detailing that the Security Analyst position was "too much" for him. He sent the email on August 30, 2011, and his request was "approved like almost instantly".

46. Grievant testified, believably, that it was his understanding that he was being given a "voluntary demotion" back into his Network Engineer position.

[11] Grievant explained that he was required to review and "check out" equipment for vendors and the departments. Consequently, Grievant had equipment sitting around his small office space. Windberry agreed that there was "just a lot of equipment, tested equipment…that was being used, kind of spread out through his work area." Windberry went on to say that "a lot of the equipment was related to projects that [Grievant] was involved in that were…ongoing." Grievant stated, credibly, that he tried to "clean it up as best [he] could."

47. CIO Keil directed Deputy CIO Le Ann Tinker to meet with Grievant regarding the "demotion". During the meeting, Grievant again "requested a voluntary demotion".

48. However, when Ms. Tinker informed CIO Keil of Grievant's request for a "voluntary demotion", CIO Keil refused to accept or characterize Grievant's demotion back into his old Network Engineer job as a "voluntary demotion".

49. Some later time, Grievant learned from Human Resources that his resumption of his old Network Engineer position was recorded as a "disciplinary" or "non-voluntary" demotion.

50. Neither Susan Dubose, in the City's Human Resources department, nor Nancy Ortega, Administrative Support Specialist for the IS department, were clear on whether or not Grievant's demotion was "voluntary" or "non-voluntary". In fact, as evidenced by their e-mails, both Ms. Dubose and Ms. Ortega believed the demotion was "voluntary".

51. Ms. Dubose (Human Resources) emailed Mr. Keil and Ms. Tinker, along with Ms. Ortega (Information Systems), on August 31, 2011 and asked regarding Grievant: "Voluntary demotion?" On September 1, 2011, Ms. Ortega (Information Systems) wrote back a reply to Ms. Dubose (Human Resources): "Yes. Sorry I forgot to specify that. Do I need to send an updated assignment change? I also have his [Timon's] letter stating it is voluntary, but I thought they sent you a copy."

52. On September 2, 2011, IS Administrative Specialist Ortega sent yet another e-mail to Ms. Dubose (Human Resources) regarding Grievant's demotion: "Just found out it should not be considered voluntary."

53. At the contested case hearing, it was unrebutted that Grievant's demotion was reported as a "voluntary demotion" at the Chattanooga City Council meeting.

54. Additionally, it is judicially or "officially" noticed pursuant to §10.03, RESOLUTION NO. 26612 OF THE CITY COUNCIL OF THE CITY OF CHATTANOOGA, that the City Council's September 6, 2011 minutes state:

> Information Services: "**MARK TIMON—**Voluntary Demotion to Network Engineer, Range 20, $57,680.00 annually, effective 8/30/11.

55. Considering all of the above facts, the evidence preponderates that Grievant's demotion was, in fact, "voluntary" rather than "disciplinary".[12]

56. On the same day that Grievant resumed his Network Engineer position, August 30, 2011, Brent Page was placed into the "Security Analyst (acting)" position.[13]

*City "Network Passwords"*

57. According to Network Manager Windberry, Grievant was given the "new" City network passwords during the first part of September, 2011 (around a week after Grievant resumed his "Network Engineer" position), because the network team was "going to be behind" and the team needed Grievant to perform his job as a Network Engineer.

---

[12]Whether or not Grievant was "demoted" as discipline is not relevant to the issue of whether or not Grievant committed the alleged acts which led to his termination. However, whether Grievant's demotion was "voluntary" at Grievant's request, or whether it was "disciplinary" and imposed against Grievant's wishes, is relevant for the purpose of determining: (1) whether "progressive discipline" was followed by the City when Grievant was terminated, and (2) the appropriate discipline in this case.

[13] Mr. Page testified that his Security Analyst duties differed from Grievant's duties as Security Analyst because Page was "explicitly told that [he was] not a project manager." The Security Analyst position also changed after Page assumed the SA duties because Mr. Page did not have to physically install security cameras. Nor did Mr. Page do any network assessments. Mr. Page testified that he does not have access to "network passwords" because he does not need them in his job as Security Analyst, nor has he been certified to operate certain network devices such that he could use "network passwords".

58. By IS policy, only four individuals in the IS Department are given the City's "network passwords". The current City "network passwords" allow the IS Network team to access the City's computer network for the purpose of managing and configuring switches, routers, network gear and equipment, and data traffic. Not even the CIO, Mark Keil, possesses the City "network passwords".

59. "User passwords" are passwords which allow an individual user to log onto their computer and access the network. Each "user" in a network has a different "user" password.

60. "Network passwords" are administrative passwords which allow a Network Engineer or administrator to program or manage the entire network's infrastructure. An individual possessing a "network password" would be able to manage and configure all the network equipment, gear, switches, routers, firewalls, etc., throughout the entire City.[14]

61. The City's "network passwords" are long and consist of a variety of case sensitive letters, numbers, and symbols.

62. According to Network Manager Jerod Windberry, usually the network passwords are generated in a form that will have numbers, letters, symbols, uppercase, and lowercase letter. Windberry tries to make new "network passwords" 14 to 16 characters long.

---

[14] It should be also be noted that the network "infrastructure" includes physical hardware used to interconnect computers and users, the transmission media, including telephone lines, cable lines, along with routers (which route or send network traffic to all machines and gives each computer on the network an IP address for communication, and decides where the data goes), aggregators, repeaters, wireless, and other devices that control transmission paths within the network. Network "infrastructure" also includes the software that is used to send, receive, and manage signals or data that is transmitted. A person that has access to a router can divert data.

63. The "network passwords" are generated by either Jerod Windberry or someone on the "network team." According to Mr. Windberry, if an employee leaves the network team, the "network passwords" are changed to new passwords.

64. Once the four "network password" employees on the network team have been given the new network passwords, they are instructed to memorize the passwords. According to CIO Keil and Technical Manager Windberry, it is an unwritten policy that the City employees who possess "network passwords" are not to write down the passwords or store them in an unsecure place. It is understood that the "network passwords" are to be kept in a highly confidential fashion.

65. According to Technical Manager Windberry, it is not an accepted practice to give out "network passwords".

66. As a general rule, the IS Department changes the "network passwords" every 90 days. According to CIO Keil, the "user passwords" are also changed every 90 days.

67. The City's Information Policy (hereinafter the "IS Information Policy") concerning IS employees' access to City computer passwords was signed by Grievant in the year 2000.[15]

---

[15] The city attempted to introduce a new IS Policy which was adopted on September 13, 2011 (during the meeting described below) as the Policy which was in effect at the time of the "Dropbox incident". Grievant objected to the introduction of the new September 13, 2011 policy on the basis that the new policy was not in effect and did not govern Grievant's acts which comprised "the Dropbox incident." The undersigned agrees. The new IS policy which went into effect on September 13, 2011 was excluded from evidence as not being the governing policy at the time Grievant "dragged" confidential network passwords into a "Dropbox." The new September 13, 2011 Policy is not relevant and was excluded from evidence.

On September 13, 2011, the IS Department had a meeting with all IS employees to address "access to accounts, and data, and devices…who should and should not have access to that, and that there were strict disciplinary considerations of policy." The meeting was conducted by Jana Lowery, Applications Service Manager for Chattanooga's IS Department. According to Ms. Lowery, the meeting did not

68. The IS Information Policy *(Policy Governing Information Services Staff's Access to City of Chattanooga Data*)[16] states as follows:

> Only those personnel in the exercise of their normal, authorized assigned duties and responsibilities shall attempt to access ANY data in any form belonging to the City of Chattanooga. Some examples are Account Files, Network packets, application inquires (sic), email, temporary data files on user PC, listings, Network Files or Data Files etc. That access shall be for a specific stated purpose, authorized, supported by an appropriately authorized work document and assigned to a specific individual. Work performed and information gained as a result of this access shall not be shared or distributed except as intended and stated by the authorizing work document.
>
> Violation of this policy shall be dealt with in a manner proportionate to the seriousness and intent of the violation. Disciplinary action against the violating individual(s) will be considered ranging from a reprimand up to and including dismissal.

69. At the time the IS Information Policy was adopted, many networks and current web servers/computers were not in existence. As an example, neither "Facebook" nor "Dropbox" accounts existed in the year 2000; and many of the cell

---

specifically address the security of passwords. Testimony concerning the September 13, 2011 meeting and the adoption of the "new policy" is not relevant to Timon's inadvertently placing "network passwords" into a Dropbox file *prior to the meeting and prior to the adoption of the new policy.* Accordingly, such evidence is not considered.

[16] Grievant argues that the IS Information Policy set forth above (which was signed by Grievant in the year 2000) does not apply to this case or this set of facts because it is "outdated". Grievant points out that the term "password" is not used in the IS Information Policy. Pursuant to the IS Information Policy set forth above, Grievant had "permission" and the "authority" *to possess* the "network passwords." The IS Information Policy is the policy which was in effect at the time of Grievant's "Dropbox incident". The City's argument that Grievant "violated" the "Policy" by simply setting up a "Dropbox account" because Grievant did not have the "authority" to set up a Dropbox, for the purpose of sending photographs of a joint Excalibur- City security project, is without merit. Clearly, Grievant had the "authority" within the course and scope of his employment as the City's "Security Analyst" to send data files (such as photographs) to a City contractor (Excalibur) for the purposes of working on a joint project assigned and authorized by the City. Grievant was one of the "authorized" IS employees who had been given "network passwords". It is also apparent that Grievant did not intentionally share confidential City data with his contact at Excalibur. For this reason, the undersigned disagrees with Grievant that the IS Information Policy does not apply to this case. However, under the plain wording and meaning of the IS Information Policy, Grievant did not violate the Policy.

phones which can receive and transmit data files and emails did not exist in the year 2000.

70. According to ICO Keil, the IS Information Policy was adopted just to "govern the authorization procedures of publishing technology." The Policy itself gives "examples" of account files, network packets, application inquiries, e-mails, temporary data, network files, data files.

*The Dropbox Incident*

71. While Grievant was employed in the position of Security Analyst, Grievant worked with third-party vendors who contracted with the City of Chattanooga.

72. One of the third-party vendors Grievant was required to work with, within the course and scope of his position as the Security Analyst, was Excalibur Integrated Services ("Excalibur"), an information technology consultant based in Chattanooga, Tennessee.

73. Grievant was assigned to work with Excalibur on the Police Department's interior/exterior camera project. The Police Department cameras' purpose was to monitor fencing, alarm systems, surveillance systems, and other City of Chattanooga property. The project included performing a "security analysis" for the purposes of improving the security camera system. Excalibur was the consultant or vendor who had contracted to provide the equipment for the "police camera project".

74. The City of Chattanooga's computer network does not allow computer users to attach and send data files by email if such data/data files are greater than 10 megabytes in size.

75. Dropbox is a file sharing program that is available free of charge on the Internet for the purposes of "dropping" files or data into it by "dragging" a file into Dropbox. A "link" to the Dropbox is set up, and a "user password" is given to individuals intended to access the Dropbox. Thereafter, the data in the Dropbox can be retrieved by individuals who have been given access (the link plus the user password) to that particular Dropbox.

76. In June, 2011 Grievant Timon had taken various photographs of police security cameras which he needed to share with Excalibur for purposes of their working together on the "police camera project". Grievant and the Excalibur contact person (Bobby Bullington) had done a "site visit", and Grievant had taken photographs of the existing police camera locations.

77. Because Excalibur did not have any its employees "on site" at the City IS offices, and because Mr. Timon wasn't traveling to Excalibur's offices in the near future, Grievant decided to forward the security camera photographs via computer to his Excalibur contact, Mr. Bullington. Grievant Timon had twenty-five or thirty photographs which he needed to send to Mr. Bullington.

78. Due to the large file size of the photographs (in excess of 10 megabytes), Grievant could not attach the photographs to an e-mail and send them to Mr. Bullington.

79. For this reason, Grievant Timon decided to set up a "Dropbox" account, place the copies of the photographs into the "Dropbox" file, and share the file (link and user password) with Mr. Bullington at Excalibur.

80. Mr. Bullington was the only recipient of the "Dropbox link" set up by Grievant.

81. At some unknown time Grievant created a "confidential.pdf" file (unrelated to the "Police Camera Project") on his personal laptop computer. The file was encrypted and required a password for access.

82. Grievant Timon testified, credibly, that he had never been instructed by anyone at IS that he could not keep a record of "passwords" on his personal computer. According to Mr. Timon, he would typically save a new "password" into the "confidential file" on his personal computer which was encrypted and password-protected. Timon explained that it took a while to memorize a 16-character password containing special characters, numbers, lowercase letters, and uppercase letters.

83. Grievant testified, believably, that "it [the network password] is not something you can look at once and remember."

84. Timon's demeanor and manner were carefully scrutinized during his testimony. He testified, credibly, that he did not intentionally put any "network passwords" into the "Dropbox" file he had set up to share the security camera photographs.

85. He further testified, convincingly, that he would never have intentionally done such a thing; and that he did not know how the "confidential.pdf" file got into the Dropbox.

86. Grievant explained that he did not remember ever putting his "confidential.pdf" file into the "Dropbox" file, and must have accidentally "dragged" or

placed his "confidential.pdf" file containing the "network passwords" into the Dropbox file.

87. Grievant expressed great remorse for his mistake.

88. Clearly, Grievant's placing a file marked "confidential.pdf" which contained his personal email information, his personal banking records, and the City's "network passwords" was not a file he intended to share with anyone else.

89. Grievant's error was discovered by accident.

90. Sometime after August 30, 2011 (when Grievant Timon had resumed his "Network Engineer" position, and Brent Page had been promoted to the "Security Analyst (acting)" position vacated by Mr. Timon) the City's Deputy CIO/Director of Technology, Le Ann Tinker, was at Excalibur's offices for a meeting on another project.

91. While Ms. Tinker was at Excalibur, she talked with Bobby Bullington, Excalibur's Account Manager for the City's projects.[17]

92. Brent Page, the newly appointed Security Analyst, had mentioned to Deputy CIO Tinker that he needed copies of the photographs which Excalibur and Grievant had been using to work on the "police camera project".

93. When Ms. Tinker relayed this information to Mr. Bullington, Mr. Bullington offered to download the photographs Grievant had sent him for the "police camera project" onto a "flash drive."

94. Ms. Tinker took the "flash drive" containing the "police camera project" information back to the IS offices, and gave it to Mr. Page.

[17] Mr. Bullington is the "Director of Sales" for Excalibur. Excalibur holds numerous accounts with the City of Chattanooga, so Mr. Bullington has a lot of interaction with different departments within the City regarding their contracts/ projects. At all relevant times, Mr. Bullington was Grievant's "contact" at Excalibur while Grievant was working on the "Police Security Camera Project" with Excalibur.

95. At some point, the new Security Analyst, Brent Page, reviewed the information on the "flash drive" which contained the "police camera project" photographs.

96. Mr. Page e-mailed Deputy CIO Tinker to inform her that he had discovered a file on the "flash drive" entitled "Confidential. pdf". Mr. Page further related to Ms. Tinker that the "Confidential.pdf" file on the "flash drive" appeared to contain City passwords.

97. Ms. Tinker asked Chad Rowlee, a Network Analyst, to review the "flash drive" containing the "confidential.pdf" file to ascertain whether or not there were indeed City "network passwords" contained in the "flash drive's" "confidential.pdf" file.

98. When Network Analyst Rowlee confirmed to Ms. Tinker that the "confidential.pdf" file on the "flash drive" contained current City "network passwords", Ms. Tinker met with CIO Mark Keil and Mr. Rowlee on September 16, 2011 to apprise CIO Keil of the situation and discuss it.

99. After the meeting with CIO Keil, Ms. Tinker contacted the City's personnel department for guidance, and was advised to place Grievant on "administrative leave" without pay while IS investigated the matter.

100. On the afternoon of September 16, 2011, Ms. Tinker asked Grievant if he knew anything about the Dropbox account copied onto the "flash drive". That was the first time that Timon realized his "confidential. pdf" file could have been placed on the Dropbox file.

101. Grievant explained to Deputy CIO Tinker that he had created the Dropbox account for the purpose of using it to share "security camera project" photographs with Mr. Bullington at Excalibur.

102. When Tinker informed Grievant about the "network passwords" included in a "confidential.pdf" file in the Dropbox, Grievant realized for the first time that City "network passwords" had mistakenly been placed on the Dropbox file.

103. At Grievant's meeting with Ms. Tinker, he was given a letter from Ms. Tinker placing him on "Administrative Leave" without pay, and was notified that he would be given a "*Loudermill* hearing" on Friday, September 23, 2011.

104. Mr. Bullington was the only person at Excalibur who had access to the "Drop Box" file set up by Grievant. Neither Mr. Bullington nor anyone at Excalibur realized that the "Dropbox" contained the City's "network passwords" within a "confidential.pdf" file that had mistakenly been placed on the "Dropbox".

105. Mr. Bullington did not realize that Grievant had inadvertently placed "confidential information" on the "police camera project" Dropbox until Bullington was notified by City IS employees.

106. CIO Keil admitted at the hearing that City employees had given Excalibur employees "City passwords" before when Excalibur needed the passwords to work on City projects. In those situations, Excalibur employees "had permission within the project to have the passwords".

107. Additionally, according to CIO Keil, the City had also given Excalibur employees "router passwords" in the past. Some of the "router passwords" given to Excalibur allowed Excalibur employees access to entire City network.

108. CIO Keil testified that "in some cases we've [City IS employees] actually stood over the shoulder of the person from Excalibur working on project."

109. Two "current" network passwords were discovered on the "flash drive" containing the copy of Grievant's "Dropbox file".

110. Initially, CIO Keil testified that Grievant should never have set up a "Dropbox file" for the security camera photographs.[18]

111. However, CIO Keil agreed that Dropbox files are encrypted, and require a separate password to access a Dropbox file.

112. Technical Manager Windberry acknowledged that Dropbox is a "good tool for certain situations."

113. Interestingly, CIO Keil admitted that he used a Dropbox account himself when he was in Australia doing a demonstration on the City of Chattanooga's network. CIO Keil asked an IS employee to set up a Dropbox account and place the files for his presentation into the Dropbox account. Keil asked for, and was sent, the password to access and manipulate security cameras located in Chattanooga for the presentation he was conducting in Australia. The password allowed CIO Keil to remotely operate equipment in Chattanooga (turn Chattanooga park lights up and down, and operate three City security cameras.)

114. Keil conceded that "the city of Chattanooga lost control over passwords" when it sent him a password to Australia.

---

[18] As an example, CIO Keil stated that the Department of Homeland Security did not want the City of Chattanooga to send data to DHS on a Dropbox account.

115. Despite the unwritten "rule" that "passwords aren't supposed to be written down", Keil said it was acceptable to send passwords via email, store emails on a computer, or otherwise communicate passwords if there was "authorization" or "permission within the project [with third party vendors such as Excalibur]".

116. With regard to the City's password transmission and Dropbox data used in CIO Keil's Australian presentation, CIO Keil stated that he had "given [himself] authorization" for his use of the transmission of the City password and the set up and use of the Dropbox site.

117. At the hearing, the City essentially took the position that Grievant's blunder in placing his "confidential.pdf" on the "security camera project" Dropbox file (which Grievant set up for Mr. Bullington at Excalibur) exposed or "threw the door open" for anyone in the public to access confidential City data.

118. However, CIO Keil admitted that while someone with access to Grievant Timon's Dropbox file[19] would have access to the City Network, they would still need additional "passwords" or would need to "hack in" in order to get access to confidential data such as police files, juvenile files, etc.

119. While the "network passwords" on Timon's Dropbox gave the Dropbox recipient, Mr. Bullington at Excalibur, "the capability" to access or "hack into" confidential city records, the "network passwords" did not actually "open" confidential city data for the police department, fire department, etc.

120. At the time of Grievant Timon's termination, the IS Network employees who were authorized to have current "network passwords" were Windberry, Chad

[19] As noted previously, the only person Grievant Timon gave access to the Dropbox file was one person, Mr. Bullington, at Excalibur.

Rowlee (Network Analyst), Zac Cullis (Network Analyst) and Mark Timon (Network Engineer.)

121. The last time Grievant's "Dropbox account" for Mr. Bullington was "modified" was on September 9, 2011. That is also the day that Timon was given the new "current" network passwords.

122. The City of Chattanooga does not know the exact date that the "network passwords" (contained in the "confidential.pdf" file) were posted to the Dropbox. Nor does anyone with the City of Chattanooga actually know if Grievant "updated" the Dropbox with "network passwords" on September 9, 2011.

123. Technical Manager Windberry testified that he keeps a list of old "network passwords" in a list on his desktop computer in his office. The list is in a "password protected" document on his computer.[20]

124. According to Windberry, "network passwords" would not give someone unlimited access to everything in the entire network, however, it would put them a "step closer" to accessing network information. Windberry explained that is why there are additional passwords for servers, which serve as one more security step.

125. City of Chattanooga IS management, including CIO Keil, determined that Timon did not "intentionally" place network passwords on the drop box account.

126. Chad Rowlee, Network Analyst for the City of Chattanooga, testified that he was asked to review the "flash drive" copy of the Dropbox file and information contained in the "confidential.pdf" file on Dropbox file by Ms. Tinker. He *made a copy*

[20] It is noted that the City of Chattanooga has Systems Data Base Specialists who have the information and the ability to access individual computers within the City network and the information on those computers.

*of the "confidential. pdf" file* on his computer, "password locked it", and took the flash drive back to Ms. Tinker.

127. Mr. Rowlee stated that he "tend[s] to keep passwords close to…me, *if they're not actually in my head.*"[21]

128. According to Mr. Rowlee, at the time of the contested case hearing, he still had a copy of the "confidential.pdf" file on his computer.

129. Mr. Rowlee admitted that he "tries to memorize" the confidential network passwords "very soon" after receiving them. Rowlee acknowledged that he did write down the passwords to "disseminate them to the other network people that would need those passwords."[22]

130. No actual harm resulted to the City of Chattanooga due to Grievant's mistakenly placing the "confidential" "network passwords" on the Dropbox file.

131. Network Analyst Rowlee[23] testified that he changed all the "network passwords" on the date (September 16, 2011) the "confidential.pdf" file was discovered on the "flash drive" copy of the Dropbox file.

132. CIO Keil called each Department Head in the City, along with external agencies who interfaced or used with the City's network, to inform them of the potential problem and to advise them of the steps that would be taken to limit the possibility of the City's security exposure.

---

[21] The logical conclusion is that if "network passwords" are "not actually in [Rowlee's] head", such "network passwords" are recorded, written down, or stored in a data file.
[22] The City's argument that the four current "network passwords" are never written down or stored, but are always immediately memorized, is not deemed credible and is rejected.
[23] Mr. Rowlee was "Acting Network Manager" due to Network Manager Windberry's absence from work due to Mr. Windberry's taking military leave.

133. After the "network passwords" were changed by Mr. Rowlee, the City used a network auditor (outside consultant) to check every device on the network to make sure it was not compromised.

134. There was no compromise of confidential city data.

135. The City had to pay the consultant approximately $3000 to conduct the security check on each city device.

136. It is noted that the City of Chattanooga had obtained network audits by the same consultant on previous occasions.

*Loudermill ("Due Process") Hearing*

137. CIO Keil assigned or designated Deputy CIO Le Ann Tinker to conduct the "*Loudermill*" (due process) hearing" for Grievant.[24]

138. CIO Keil prepared the "termination letter" terminating Timon from employment prior to the "Due Process" hearing, and instructed Ms. Tinker to give it to Timon at the end of the "*Loudermill* hearing".

139. At the "*Loudermill* hearing" Grievant was extremely remorseful, embarrassed, and apologetic over his careless mistake.

140. Grievant explained to Ms. Tinker why he set up the Dropbox, and stated that he did not intentionally place "network passwords" in the Dropbox.

141. Grievant further explained that he did not realize his "confidential.pdf" file had been placed in the "police camera project" Dropbox until Ms. Tinker brought it to his attention on September 16, 2011.

[24] At all relevant times, Ms. Tinker was Deputy CIO/Technical Manager of the City's IS Department. However, Ms. Tinker was demoted to another position in December, 2011.

142. CIO Keil's testimony that he had not entirely decided to terminate Grievant prior to the "due process" hearing is not deemed credible.

143. The fact that the decision was made to terminate Grievant prior to Grievant's being allowed to respond to charges at the "*Loudermill* (due process) hearing" is further demonstrated by the conflicting dates on a September 29, 2011 e-mail sent by Nancy Ortega (Administrative Support Specialist, IS) to the Chattanooga Personnel department with the subject of "Timon termination", the attachment of "HR TERMINATION Sept 10, 2010), and the message in the e-mail stating: "He [Timon] has been sent a certified letter by mail to return all equipment by 9/23/2011."

144. The "*Loudermill* (due process) Hearing" was scheduled and held on September 23, 2011.

145. Neither party admitted into evidence a "certified letter" which had been sent to Mr. Timon to "correct" the e-mail or state any different information than that contained in the September 29, 2011 e-mail from Ms. Ortega.

**Conclusions of Law**

1. The City of Chattanooga bears the burden of proof in this matter to show that Grievant was (1) inefficient or negligent in the performance of his duties; and/or (2) violated the City of Chattanooga Information Services' "Policy Governing Information Staff's Access to City of Chattanooga Data" (2000). The City also bears the burden of proof to show that the discipline imposed is the appropriate discipline for any such violations.

2. The CHATTANOOGA CITY CODE, §2-174 provides, in pertinent part:

> (a) No City employee shall be demoted, suspended or dismissed for…any…unjust or arbitrary cause.[…]

(b) Disciplinary action up to and including dismissal may be taken for any *just cause* including, but not limited to, the following:

***

(3) Inefficiency or negligence in the performance of one's duties;

***

(5) Violation of department or city ordinance(s), rule(s), regulations(s) or law(s) or violation of any applicable state law, rule or regulation subject to the provisions of this Code.

3. The evidence preponderates that Grievant inadvertently "dragged" a confidential.pdf file containing his personal banking records, his personal email information, and current City "network passwords" into a Dropbox file.

4. The City failed to show that Grievant's placing such confidential "network passwords" was intentional.

5. The evidence preponderates that other IS employees, including CIO Keil, Network Manager Windberry, and Network Analyst Rowe, have e-mailed "passwords"; have shared passwords, including router passwords, with third parties working on city projects; and have written down, recorded, or stored "network passwords" until they have memorized such passwords; have used Dropbox accounts.

6. The question must be asked: Should Grievant be penalized or disciplined for storing City "network passwords" on his password-protected PC when the evidence preponderates that other City "Network Team" employees have written down, recorded, or stored "network passwords"?

7. The old axiom, "What is good for the goose is good for the gander" is applicable in this case. Grievant's creation of a Dropbox account, and Grievant's

storing his "network password" on a confidential file on his password-protected personal computer, are acts which other IS employees have committed without consequence or discipline.

8. The City did not show that Grievant was habitually careless, or made "blunders" or "mistakes" in misplacing files on his computer. In fact, the evidence preponderated that Grievant was conscientious and "security conscious."

10. No harm came to the City as a result of Grievant's blunder. No confidential City information from the Police Department, the Fire Department, etc. was actually accessed by third-parties. In short, the City of Chattanooga's computer network was not, in fact, compromised.

11. While the City argued that Grievant was not "authorized" to set up the Dropbox account to share information with Mr. Bullington at Excalibur, the City's argument must fail because Grievant was a Security Analyst who was authorized to share necessary project information on a project he and Mr. Bullington were working on. It goes without saying that Grievant had permission to supply Mr. Bullington with information and photographs both parties needed in order to work on a joint, contracted security camera project between the City and Excalibur.

12. The evidence does not preponderate that Grievant was "grossly negligent" by inadvertently moving a personal file into his Dropbox file.

13. Had there been a scintilla of evidence that Grievant *intentionally* shared City "network passwords" with anyone not authorized to possess such "network passwords", this matter would have a very different outcome. That is not the case.

Grievant did not intentionally share "network passwords" with Mr. Bullington or anyone else.

14. The Grievant did not violate the IS Information Policy by setting up a Dropbox file to share the security camera photographs.

15. Accordingly, Grievant's only "violation" is his violation of CHATTANOOGA CITY CODE, §2-174 (b)(3) for "negligence".

16. The City has not shown, by a preponderance of the evidence, that it has "just cause" to terminate Grievant.

17. Accordingly, the questions which must be answered below are: (1) Were Grievant's due process rights violated; and (2) What is the appropriate discipline for Grievant's one act of negligence?

*Due Process*

18. The 14th Amendment to the United States Constitution protects individuals against government deprivations of "life, liberty or property without due process of law.

19. Because City of Chattanooga employees have "property rights" in their jobs; such employees must be afforded constitutional due process before the City may legally deprive the employee of his job. *Hinson v. City of Columbia*, 2007 WL 4562886 (Tenn. Ct. App. 2007).

20. Grievant was provided with a "*Loudermill* (due process) hearing" on September 23, 2011.[25]

[25] The term "Loudermill hearing" arises from the United States Supreme Court decision in *Cleveland Board of Education v. Loudermill*, 470 U. S. 532 (1985).

21. The evidence preponderates that CIO Keil's decision to terminate Grievant was made prior to Grievant's "*Loudermill* hearing". The "termination letter" was drafted prior to the "*Loudermill* hearing."

22. Pursuant to the decision in *Cleveland Board of Education v. Loudermill,* 470 U.S. 532, 546 (1985), a public employee who can only be discharged for cause *must be given notice and an opportunity to respond to the charges prior to his termination.* (Emphasis added.)

23. Procedural due process does not require "perfect, error-free governmental decision making." *Qualls v. Camp*, 2007 WL 2198334 *4 (Tenn. Ct. App. 2007.) However, it does require affording a civil service employee a "relatively level playing field." Id. at 4.

24. A recording of the "*Loudermill* Hearing" was played during the contested case hearing of this matter. Without much ado, Ms. Tinker informed the individuals present that the "this is being recorded." She then instructed Grievant: "Mark, this is your opportunity to address the situation, so you can talk."

25. Grievant responded:

> The only way, and what I can think of that happened …is I had the Dropbox account as a share, mapped on my PC, and I inadvertently drug it over there and copied it over there. I do not remember putting it out there. It was a mistake on my part that I made. I understand it was a, a bad mistake. […]As soon as you guys notified me that it was out there…I went in and talked to Chad [Rowlee] to tell him how to…change the passwords to…secure it from that point on.
>
> ***
>
> […] I beg for forgiveness, say it will never happen again…[.]

26. There is no evidence that any information Grievant provided at the *Loudermill* hearing was considered prior to the decision to terminate Grievant. Other

than telling Grievant "This is your opportunity to address the situation, so you can talk", no questions were asked by the designee conducting the *Loudermill* hearing. There is no evidence that the designee communicated the results of the *Loudermill* hearing to CIO Keil before handing the termination letter to Grievant.

27. Prior to the termination of a public employee who may be terminated only "for cause", the employee must be given notice of the charges against him and afforded an opportunity to respond to such charges. *Case v. Shelby Co. Civil Serv. Merit Bd.*, 98 S.W. 2d 167, 170 n.1 (Tenn. Ct. App. 2002), citing *Cleveland Bd. of Education v. Loudermill,* 470 U.S. 532 (1985). See also *Redmon v. City of Memphis*, 2010 WL596385 *7 (Tenn. Ct. App. 2010).

28. However, even if it is concluded that Grievant was not afforded proper "due process" prior to the decision being made to terminate Grievant, and even if the "*Loudermill* hearing" was held as a mere formality, Tennessee case law is replete with cases which make it clear that a *de novo* hearing with a full and complete opportunity for a Grievant to be heard "cures" any prior lack of due process. See *Redmon v. City of Memphis*, 2010 WL596385 *7 (Tenn. Ct. App. 2010); *McLeay v. Metropolitan Hospital Authority,* 2008 WL 4963520 *3-4 (Tenn. Ct. App. 2008).

29. Accordingly, any due process deficiencies have been rendered **MOOT** and have been "cured" by the *de novo* contested case hearing held in this matter, which afforded Grievant a full and fair opportunity to adjudicate this matter in a neutral forum. Grievant's "due process" argument is **MOOT** and must be dismissed.

*Appropriate Discipline*

30. Having concluded that Grievant committed the negligent act of placing "network passwords" into a Dropbox file shared with an Excalibur employee, the final question which must be asked is: What is the appropriate discipline for Grievant?

31. Tennessee's Civil Service statutes and rules incorporate the doctrine of progressive discipline. Accordingly, government employers are expected to administer discipline beginning at the lowest appropriate step. *Kelly v. Tennessee Civil Service Commission*, 1999 WL 1072566 (Tenn. Ct. App. 1999). Further, at least one court, in expressing approval of the progressive discipline system, has stated that the legislative mandate for progressive discipline should be "scrupulously followed". *Berning v. State of Tennessee, Department of Correction*, 996 S.W. 2d 828, 830 (Tenn. Ct. App. 1999).

32. An employee's prior conduct, both good and bad, along with his entire work history, can be considered when determining what the appropriate disciplinary action should be. *Kelly v. Tennessee Civil Service Commission*, 1999 WL 1072566 (Tenn. Ct. App. 1999).

33. There was no evidence entered that Grievant's entire work history or any performance evaluations were considered by CIO Keil for purposes of deciding the appropriate discipline for Grievant. No performance evaluations were entered into evidence.

34. Three prior disciplinary actions were taken against Grievant in 2004 (three day suspension without pay for below standard performance), 2005 (one week suspension for "unsatisfactory performance"), and 2006 (three day suspension without pay for failure to follow IS's quality assurance policy).

35. The evidence preponderates that Grievant's work performance thereafter was extremely good. In fact, Grievant's performance was good enough that he got a promotion in January, 2011.

36. The City argues that Grievant's "demotion" was an "involuntary disciplinary action" against Grievant in August, 2011, and wants such "demotion" to be considered a "strike" against Grievant in this proceeding.

37. However, the evidence preponderates that Grievant thought the Security Analyst position was "too much" and "overwhelming", and Grievant requested the demotion.

38. Further, credible testimony given by Deputy CIO Tinker supports that Grievant worked hard in his new position of Security Analyst, and "was attempting to do the work successfully."

39. It is determined that the "demotion" back into Grievant's previous position as "Network Engineer" was voluntary. For this reason, Grievant's resumption of his previous position cannot be considered "discipline" against Grievant.

40. "Termination" for one act of negligence, albeit a serious act of "negligence" in light of Grievant's past work history, does not support that "progressive discipline" was utilized with Grievant.

41. An additional consideration for determining the appropriateness of the discipline to be imposed is whether the punishment imposed upon the Grievant is different than discipline used with other employees who have engaged in the same conduct. *Gross v. Gilless*, 26 S.W. 3d 488, 495 (Tenn.Ct. App. 1999), *Perm. to Appeal Denied* (Tenn. 2000).

42. Grievant introduced evidence that showed other employees who had *intentionally* given out confidential City passwords were NOT terminated for such actions.

43. Dan Collier, a previous Network Administrator, placed/used the "systems administrator password" on a "loaner" computer which was used by and accessible to numerous City employees. He was not disciplined and was not terminated for exposing the City's network password.

44. Alexander Bentley, a former IS employee of the City, gave out the City's "network password" during a meeting with a third party vendor for the city and other employees. The vendor had the "network password" actually written down on a piece of paper. Mr. Bentley did not receive discipline, nor was Mr. Bentley terminated for communicating the "network password" to others, including third parties.

45. The "standard" for discipline in this case is set forth in RESOLUTION NO. 26612 OF THE CITY COUNCIL OF THE CITY OF CHATTANOOGA, §9, which provides that there must be "cause" for the disciplinary action and a "reasonable basis" for the employment decision.

46. After considering the totality of the circumstances in this matter, including past discipline, Grievant's employment history and record, and all the facts and circumstances in this case, it is determined that the appropriate discipline in this matter is a ninety (90) day suspension without pay.

47. Termination is too harsh for Grievant's one act of negligence in inadvertently "dragging" a personal confidential file into the Dropbox file shared with Mr. Bullington.

48. The City did not show that actual harm occurred to the City's network, or that the network had been breached as a result of Grievant's negligence.

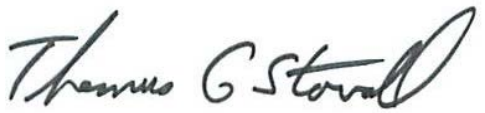
49. However, the seriousness of Grievant's negligence in this matter supports a significant suspension in this matter. Sufficient discipline is necessary to ensure that Grievant will be extremely cautious and vigilant in his work for the City, and will not make such an error in the future.

For all the above reasons, and considering all the facts and circumstances of this case, and the record as a whole, it is determined and **ORDERED** that the appropriate discipline for Grievant's "mistake" or "negligence" is a ninety (90) day suspension without pay from *September 23, 2011 until December 22, 2011*. Grievant shall be reinstated to his position as a Network Engineer with the City, and shall be made whole with regard to benefits, seniority, and lost wages (after the deduction of the 90 day suspension without pay).

Pursuant to RESOLUTION NO. 26612 OF THE CITY COUNCIL OF THE CITY OF CHATTANOOGA, §12, the policy reasons for this decision are to uphold the public's and the government's interest in consistent civil service policies and procedures, and to ensure that City actions are carried out in accordance the City's Charter and other applicable laws.

It is so ordered.

This Final Order entered and effective this 14 day of February, 2012



Thomas G. Stovall, Director