Notice: This decision may be formally revised before it is published in the *District of Columbia Register* and the Office of Employee Appeals' website. Parties should promptly notify the Office Manager of any formal errors so that this Office can correct them before publishing the decision. This notice is not intended to provide an opportunity for a substantive challenge to the decision.

THE DISTRICT OF COLUMBIA

BEFORE

THE OFFICE OF EMPLOYEE APPEALS

In the Matter of:)
)
EMPLOYEE,) OEA Matter No. 1601-0001-21
)
) Date of Issuance: May 17, 2023
v.)
) JOSEPH E. LIM, ESQ.
OFFICE OF THE ATTORNEY GENERAL,) Senior Administrative Judge
Agency)
Charles Tucker, Esq., Employee Representative
Jhumar Razzaque, Esq., Agency Representative

INITIAL DECISION

INTRODUCTION AND PROCEDURAL HISTORY

Employee filed a Petition for Appeal with the Office of Employee Appeals ("OEA" or "Office") on October 5, 2020, challenging the District of Columbia Office of the Attorney General's ("Agency" or "OAG") decision to terminate him from his position as an Information Technology Specialist for the following causes: (1) Neglect of duty, and (2) Misconduct. After OEA requested an answer on March 5, 2021, Agency filed its Answer on April 12, 2021. Following Agency's refusal to participate in mediation on May 28, 2021, this matter was assigned to the undersigned Senior Administrative Judge ("SAJ") on July 1, 2021.

Based on the parties' availability, a Prehearing Conference was held on September 9, 2021, and discovery was completed on October 31, 2021. After a Consent Motion filed by the parties for postponement, another Prehearing Conference was scheduled for January 5, 2022. A Show Cause Order was issued to Employee for failure to attend the conference and Employee responded on January 10, 2022, citing that his attorney had a medical emergency. A second conference was held on February 28, 2022, and an Evidentiary Hearing was held virtually on June 13, 2022, and June 14, 2022. The record is now closed.

JURISDICTION

This Office has jurisdiction in this matter pursuant to D.C. Official Code § 1-606.03 (2001).

ISSUES

1. Whether Agency had cause to take adverse action against Employee; and

2. If so, whether the penalty of termination was appropriate under the circumstances.

SUMMARY OF CHARGES

On September 17, 2020, Agency served Employee, an Information Technology ("IT") Specialist, a Final Decision on the Advance Written Notice of Proposed Removal based on two (2) causes.

> Cause No. 1 **Misconduct** - DPM Section 1605.4, 6B DCMR 1605.4, Conduct Prejudicial to the District, Unauthorized disclosure or use of (or failure to safeguard) information protected by statute or regulation or other official, sensitive or confidential information. (Counseling to removal for the first offense).
>
> Cause No. 2. **Neglect of Duty**: Failing to carry out official duties or responsibilities as would be expected of a reasonable individual in the same position; careless work habits. [See DPM Section 1605.4(e); 6B DCMR 1605.4(e) & 1607.2, Failing to carry out official duties or responsibilities as would be expected of a reasonable individual in the same position.

Specifically, Agency alleges that in the course of transferring text messages from Chief Operating Officer Penelope Thornton Talley's ("Talley") old cellphone to a new model cellphone, Employee purposefully searched for his name in Talley's text messages and then forwarded them to Chief Information Officer Tonjes to confront him. Agency charges that Employee abandoned his fiduciary role as an IT Specialist to access sensitive and confidential email and text messages sent by OAG employees. Agency asserts that protecting sensitive and confidential information is at the heart of Employee's duties and responsibilities.

SUMMARY OF TESTIMONIAL AND DOCUMENTARY EVIDENCE

On June 13, 2022, and June 14, 2022, a virtual Evidentiary Hearing was held via WebEx.[1] The following represents a summary of the relevant testimony given during the hearing as provided in the transcript (hereinafter denoted as "Tr.") which was generated following the conclusion of the proceeding. Both Agency and Employee presented documentary and testimonial evidence during the hearing to support their positions.

Christopher Tonjes ("Tonjes") June 13, 2022 Tr. Pgs. 26-136.

Tonjes was employed as a Chief Information Officer with the Office of Attorney General ("Agency"). He oversaw the Information Technology ("IT") department and was responsible for

[1] WebEx is a software program that enables participants to engage in a hearing or meeting remotely via an electronic device.

the full spectrum of technology for Agency including provisioning for telephones, mobile phones, computers, software development, and IT security. Tonjes identified Agency's Exhibit 7, Bate-stamped Number 190, and explained that it was the Office of the Chief Technology Officer ("OCTO") internet access and use policy. He explained that the purpose of the policy was to clarify when it was permissible to access the internet. Tonjes further explained that the policy was applicable to the procedure for transferring text messages from one cell phone to another. Moreover, the policy provided that an employee is not to use the internet for personal and non-D.C. government business.

Tonjes testified that the OCTO policy had been in place since 2005. He further stated that an employee did not have a reason to review, read, share, or spot check individual text messages as it was not part of an IT Specialist's duties. Tonjes testified that Employee was responsible for maintaining and supporting Agency's Legacy Citrix environment. Additionally, Employee was responsible for Justis, a criminal justice information portal that Agency used to contribute data, and he was the point of contact for Case File Express, which is the electronic filing system used by the D.C. Superior Court. He also explained that Employee was the VMware administrator, which was the virtualization software used to manage physical servers.

Tonjes stated that Employee conveyed to him that he had derogatory evidence from Tonjes, but at the time, Tonjes did not understand what Employee meant. Tonjes searched his emails and when he failed to find any derogatory evidence, he asked Employee to show him what he was referring to. Employee emailed Tonjes pictures of a phone with text messages of a conversation between Penelope Talley ("Talley") and Tonjes. Tonjes testified that he did not provide Employee guidance on sending the evidence that Employee claimed that he had. He stated that he immediately called Talley to let her know that her phone had been compromised. Tonjes was inclined to inform Talley that the phone may have been compromised because he was unsure of any other sensitive information that Employee may have seen.

After Tonjes met with Talley, they had a conference call with the Chief Human Resources Officer, and the Director of Personnel, Labor, and Employment Division ("PLED"). Tonjes stated that all parties believed that Employee's action was a serious breach of protocol. Thus, conduct prejudicial to the District Government and the neglect of duty charges were deemed appropriate adverse actions against Employee.

Tonjes testified that when he was initially hired, he was told that many of the litigators at the Agency did not want to share information because they were unsure if sensitive information would ultimately be leaked. He explained that if the public knew that people in IT were browsing through data, and using it for their own personal gain, it would hinder the trust that was given to the IT department, which was to represent and safeguard sensitive data. Because Tonjes lost his trust with Employee, he no longer felt that Employee could administer the system or passwords to amend high-level systems.

Agency's Exhibit 1, provided that the text messages shown to Tonjes by Employee were dated September 6, 2019, five months prior to Employee emailing the picture on February 19, 2020. Tonjes testified that there is no need for any employee to search for messages when they are syncing a client's phone. He also stated that he was mortified that a private conversation was breached. He explained that the text thread pertained to him asking Talley to postpone a meeting. Tonjes explained that he wanted to gather the staff to address any issues within the department. The second part of the text message stated that Employee was on a war path and enlisted the help of other employees. Tonjes stated that he and Employee had a contentious meeting. Employee complained to Tonjes that the contractors were given favorable work assignments when he and other employees could do the work that the contractors performed. Tonjes further stated that at least twice before the meeting with Employee, there was discussion with the union about whether Agency was violating the Collective Bargaining Agreement ("CBA") by hiring contractors if there was overlapping work.

Tonjes did not initially take disciplinary action against Employee because he thought that Employee might be enlisting other members of the IT team to complain in the listening session with the Attorney General. Tonjes testified that while there is no policy prohibiting the viewing of text messages, the IT division created a separate set of policies incorporating some of OCTO's policies for Agency. Moreover, Tonjes stated that based on his professional experience, text messages were not attached to an email and that it would be unlikely that an individual would be able to attach text messages to an email without having viewed the message. He opined that if the text messages were accessed, viewed, and used to confront him for personal benefit, he believed that it was possible for other confidential messages to be distributed by Employee. While Tonjes was not the Deciding Official in Employee's matter, he agreed with the deciding official's decision to terminate Employee.

<u>Jason Downs ("Downs") June 13, 2022, Tr. 137-193.</u>

Downs was employed as a Shareholder with Brownstein, Hyatt, Farer, and Schreck. Prior to this position, he served as the Chief Deputy Attorney General. He testified that Talley was one of his direct reports as his Chief Operating Officer ("COO"). Thus, anything that pertained to IT and HR went through Talley. Downs testified that the investigation of the Employee proved that there was a breach of confidential information, and he could no longer trust Employee. Therefore, it was recommended by the Attorney General ("AG"), Karl Rancine, that Employee be terminated pursuant to conduct prejudicial to the District government and neglect of duties, specifically failing to carryout official duties or responsibilities in the same position, and Downs supported the decision of the AG.

<u>Penelope Thorton Talley ("Talley") June 13, 2022, Tr. 194-210.</u>

Talley worked as the Chief Operating Officer ("COO") for Agency. She was responsible for the strategic oversight of all Agency operational functions, which included Human Resources, Information Technology, administration, finance, facilities, and support services. Talley testified that she met with Tonjes weekly to discuss matters related to the IT division.

Talley testified that in February of 2020, she upgraded her phone to a newer model. She explained that the data from the old phone was to be transferred to the new phone. However, when the data transfer occurred, the text messages did not transfer. Talley did not give anyone permission to review the contents of the text messages in her phone. She stated that if anyone had gone through her messages, she would have considered it a breach of confidentiality. However, she admitted that not all her emails and text messages were confidential.

Shiria Anderson ("Anderson") June 13, 2022, Tr. 211-262.

Anderson managed OAG's entire Human Resources ("HR") function as the Chief HR and Compliance Officer with Agency. This included performance management, classification and compensation, staffing and requirement, training and development. As it related to her role in discipline, Anderson would review the infraction that the employee was charged with against the District Personnel Manual ("DPM"). Then she would work with management to determine the level of discipline warranted.

Anderson testified that she reviewed an investigative report indicating that the contents of Talley's cell phone were compromised. A timeline of events was created of all individuals who had access to Talley's cellphone. She learned that Employee transferred data from Talley's old cell phone to the new one and accessed text messages between Talley and Tonjes. Ultimately, Anderson and higher-ups concluded that Employee had inappropriately used his position as a Network Engineer to access the text messages contained on Talley's cellphone. Anderson's recommendation to Tonjes regarding Employee was that it would be difficult to trust him moving forward, especially due to the sensitive nature of his job, and that this offense would typically result in termination. Anderson stated that Employee violated DPM section 1605 and was in violation of the OCTO policy around acceptable use.

Candyce Lovett ("Lovett") June 13, 2022, Tr. 263-295 and June 14, 2022, Tr. 199-203.

Lovett worked as an IT Specialist with Agency. She oversaw IT troubleshooting issues of network and device issues. Lovett stated that there was no written policy for the distribution of laptops and phones and that certain employees were treated differently. Lovett was informed by Tonjes and Talley that there were Very Important Person ("VIP") employees at Agency. Additionally, based on her experience, an individual would need to view the text messages to verify that the phone worked.

Lateef Sanwoola ("Sanwoola") June 13, 2022, Tr. 304-322.

Sanwoola worked as an IT Specialist with Agency. He ensured that the users of both laptops and desktops were functional and that all applications were installed properly. Additionally, Sanwoola was responsible for the data transfer of sensitive information. Sanwoola testified that Lovett walked into his office and showed him the text message between Talley and Tonjes. Lovett stated that Employee was in Tonjes's office lashing out about the text message. Sanwoola provided that Agency's Exhibit 1, Bate-stamped Number 10, was accurate, and that Mr. Sairi ("Sairi") was informed. It took Sanwoola a few hours to report the incident because he had other priorities that he was tending to.

Luke Sharkey ("Sharkey") June 13, 2022, Tr. 323-371 and June 14, 2022, Tr. 4-25.

Sharkey worked as a Contractor, specifically a Mobility Architect, with OCTO. He testified that AirWatch, a software solution program, allowed Agency to manage devices from a policy and compliance standpoint. He stated that AirWatch did not have the ability to backup or restore data. As it related to the syncing process, Sharkey stated that as a technician, he would verify if a restore was completed. He would then hand the phone to the employee and have them spot check the phone on their own because the employee would know what text messages, contacts, etc. were important, versus him going through the phone.

Sharkey testified that it was not common practice to spot check text messages to ensure that text messages transferred from one phone to another. As an IT professional, he expressed that data is king and they were not allowed to view other employee's data, as they were there to protect the data, not invade it. Sharkey explained that text messages were part of a thread, so if the text message was an older conversation, it would be collapsed. However, he did explain that if the user had a new phone and began to look through text messages, the threads may have been expanded and the message would be left on the last known state. As it related to Employee, Sharkey stated that the message was part of a thread, and the only way that Sharkey would be able to see the text was if he specifically opened the thread up to see the particular message in the conversation. He also explained that an individual would be able to use the search bar to search for a name and that would be another way to find text messages.

Sharkey testified that old text messages did not populate as new messages after a data transfer. He stated that the messages would be transferred over in the state that they were in. However, if the message was unread on the source, it would remain unread at the destination, meaning that the status would not change along the way. Furthermore, there were not multiple ways a text message could appear on a new phone during a data transfer. Sharkey further explained that the standard iPhone Operating System ("IOS") view allows a preview. If the message is part of a thread, an individual would see a partial text of the most recent message.

Employee June 14, 2022, Tr. 27-142.

Employee worked as a Senior Network Engineer at Agency. He maintained the servers, created user accounts, group policies, providing the security parameters on the systems and he served as a liaison for Courtview and Agency provided training for the Agency's own various applications. During his tenure with Agency, Employee received two performance reviews. He stated that he received stellar reviews, asserting that being proficient and efficient in his job made him a semi-perfectionist. Employee testified that when he onboarded, Agency did not have a security information system policy in place, which was why he drafted a policy and that they were not required to fall under the total umbrella of OCTO.

Employee testified that he had an interesting working relationship with Tonjes. He explained that Tonjes told the staff that he would be hiring more staff, which was greatly needed. However, instead of Tonjes hiring government employees, Tonjes hired a great deal of contractors, which caused a contentious tier situation for many of the employees already with Agency because work that would normally be under their purview was assigned to the contractors.

Employee recalled Tonjes heavily relying on him to work on special projects. Tonjes would also have Employee work with the VIP group consisting of the Attorney General, Deputy Attorney General, managers and people within the immediate office, to do tasks outside of his traditional purview. Employee was also called to help with difficult clients. Further, Employee stated that Employee's Exhibit 4-A, proved as an example of how he continued to complete work outside of his purview. He explained to Tonjes that he would not be training because it was difficult to complete his assigned tasks in addition to his other responsibilities as a senior network engineer.

Regarding how he became involved with Talley's phone, Employee explained that when Talley received a new phone, she wanted the text messages from the old phone to transfer to the new one. So, Employee assisted Talley with the transfer. He stated that he had assisted employees with their phone issues and had transferred data between the original to the new phone numerous times from the onset of his employment in 2005. Employee testified that he was hired to build a new network infrastructure for Agency. He explained that in 2005, Agency was on an antiquated data operating system, Windows NT. Part of the new infrastructure was to move the data from the old servers to the new servers.

According to Employee, in transferring Talley's text messages on the phone, he would quickly look at the messages and ensure that the data was transferring over. Employee stated that it was a quick quality assurance check to scroll and make sure that the dates coincided from the old phone to the new phone. He also stated that while he has not seen messages appear as new, in the past, Employee was aware of a breakdown of messages where a portion of the message is sent and not the entire message during the backup process.

Employee asserted that he did not intentionally scroll through to find his name on Talley's phone. He reiterated that his sole reason for going through the text messages was to ensure that the data on the old phone matched the new one, which meant that he had to scroll though the phone and make sure the dates and text messages aligned. Employee wanted Talley to have the text messages she was looking for. He also provided that if he were to move a file over from one server to another, the only way to ensure that the information was transferred to the other server was to verify the information in front of him. When Employee read the text message that read "[Employee] is on the warpath," he immediately spoke to Tonjes about it because to Employee, the message was incorrect, and he was not on a warpath. When Employee confronted Tonjes about the text message, Employee testified that Tonjes did not know what Employee was referencing until they both went into Employee's office where Employee showed Tonjes the text message. According to Employee, Tonjes asked Employee to forward the message, to which Employee obliged. Employee testified that he was unable to continue with his work and left work for the remainder of the day. Employee asserted that because Tonjes, a supervisor, requested Employee to send the message, Employee did not believe that he was partaking in an illicit act by forwarding the message to Tonjes. Employee explained that when he approached Tonjes, his intentions was not to send anything, and only showed Tonjes the message in Employee's office because he was asked to.

Employee testified that he received a notice of proposed removal in June. It was the first time that he was aware that he was charged with neglect of duty. In response to the notice, Employee argued that misconduct did not take place based on the document received from Agency; his interpretation of the term misconduct; and the actual definition. He explained that he was given a phone to fix, he fixed the issue; thus, neglect of duty did not occur.

Employee testified that he did not use AirWatch for the transfer of the text messages. However, he contradicted himself in his earlier deposition testimony on October 12, 2021, that he used AirWatch and described that he disconnected the phones from Wi-Fi and to a secure Wi-Fi using his credentials. Additionally, Employee testified that a quality assurance check would not necessarily be completed after the text messages had finished syncing and transferring. He explained that the technician could check the process periodically to ensure that the data is transferring properly. Therefore, if an issue occurred, the technician would be able to mitigate the problem at the onset of the transferring happening.

Employee stated that he received consent from Talley regarding an issue with her mobile phone and she needed the issue resolved pertaining to the text messages. Employee asserted that because he received consent to resolve any issues with Talley's phone, he had not done anything with the phone outside of the quality assurance provided to Talley. Employee maintained that he only spoke to Tonjes regarding the text that said [Employee] is on the warpath.

Jabari Garett ("Garett") June 14, 2022, Tr. 143-198

Garrett worked as a Government Contractor with the Food and Drug Administration ("FDA"). He garnered experience with assisting data transfers of laptops and cellular phones since 2012. Garret testified that if an individual received a new Apple phone, the credentials are entered, and in theory if everything is backed up on iCloud it would be synced to the new phone. He explained that he used the term in theory because there could be a phone error, bandwidth issues, or another reason. If this were to happen, a more hands-on approach would need to occur. Additionally, he testified that a portion of a message could be displayed during the synchronization process and appear as a thread or a piece of a thread. Garrett has witnessed apps that have not fully loaded, and the notifications would be shown. The read value may not have been corrected, so by default on the new phone it would be shown as a read message, which would start notifications.

As it related to notifications, Garrett explained that every app has notifications including text messages. Thus, various types of notifications could appear when data is transferred. Garrett also testified that when scrolling a message, the scroll parameters are different. He explained that one scroll could take a user to two text messages or one depending on the parameters, one scroll could take a user to fifty messages. Factors that can come into play were how the messages were grouped together by the user and sender. Additionally, if the messages were older, it could be sorted by the group name. Garrett also stated that messages did not have to be opened to see information about the text. They could be viewed by the name and some preview information across the screen.

If the messages were about four or five months prior, a user would be able to view the text messages while conducting spot checks. Garret stated that the parameters could be changed so that the oldest text message appears first so, by default, the filter in text messages specifically are shown in descending order. Additionally, to ensure that older data has come across, the setting could be adjusted so that the messages will appear in chronological ascending order, allowing the user to view the older messages, depending on how it is verified on the phone. Garrett highlighted that although they are viewing the text messages for spot checking, he did not read the messages of his clients. His goal was to ensure that the data counts are reasonable. While there is no explicit consent, Garrett stated that this method was appropriate within the federal government policies. Additionally, this method was based on data migration documents, as there is a verification step.

In the past, Garrett had performed quality checks on phones. He stated that a quality assurance check would be performed to ensure that the appropriate apps on the phone are loaded, the appropriate data, and the messages that should be there. Garrett stated that if a user used iCloud setup, the user would perform the verification from the old phone to the new phone themselves. However, if the user completed an iTunes setup, then he would help the user with the transfer and verify the data for them. When spot checking the phone, Garret stated that he would scroll to verify if the transfer worked. This method would occur after the data transfer was completed.

FINDINGS OF FACT, ANALYSIS, AND CONCLUSIONS OF LAW

Whether Agency's adverse action was taken for cause

Title 1, Chapter 6, Subchapter VI of the D.C. Official Code (2001), a portion of the Comprehensive Merit Personnel Act, sets forth the law governing this Office. D.C. Official Code § 1-606.03 reads in pertinent part as follows:

> (a) An employee may appeal a final agency decision affecting a performance rating which results in removal of the employee (pursuant to subchapter XIII-A of this chapter), *an adverse action for cause that results in removal*, reduction in force (pursuant to subchapter XXIV of this chapter), reduction in grade, placement on enforced leave, or suspension for 10 days or more (pursuant to subchapter XVI-A of this chapter) to the Office upon the record and pursuant to other rules and regulations which the Office may issue.

Chapter 16, Section 1605.4 of the District Personnel Manual ("DPM") sets forth the definitions of cause for which disciplinary actions may be taken against Career Service employees of the District of Columbia government. Employee's termination was based on:

> **6B DCMR § 1605.4, Conduct Prejudicial to the District**: unauthorized disclosure or use of (or failure to safeguard) information protected by statute or regulation or other official, sensitive or confidential information. (Counseling to removal for the first offense).
>
> **6B DCMR § 1605.4(e) & 1607.2 Neglect of Duty**: Failing to carry out official duties or responsibilities as would be expected of a reasonable individual in the same position. (Counseling to removal for the first offense).

Agency argues that Employee was guilty of misconduct, specifically conduct prejudicial to the District in that he engaged in unauthorized disclosure or use of (or failure to safeguard) information protected by statute or regulation or other official, sensitive or confidential information. Employee does not deny that he disclosed a confidential text message between Tonjes and Talley to Tonjes. Employee's defense is that he was instructed to do so by Tonjes when Tonjes initially could not recall his "[Employee] is on the warpath" text to Talley. While this is true, the evidence shows that Employee never obtained Talley's permission to disclose her text messages to anyone, even if it was to the text's author. Agency also accused Employee of failing to safeguard sensitive or confidential information when he decided to read Talley's phone text messages in the process of transferring data and text messages from Talley's old work cellphone to her new one.

Employee argues that it was necessary for him to scan and read parts of Talley's text messages for him to ascertain that these messages were successfully transferred to Talley's new cellphone, and he believed he had Talley's implicit authorization to do so when he was asked to work on the cellphones. Witnesses Sharkey and Garrett, on the other hand, testified that as IT professionals, it was an implicit part of their job to respect the confidentiality of their client's data, including text messages. I find Sharkey to be more credible than Employee when he explained that it was not necessary to read his client's data and the best person to verify whether the data was fully transferred was the client. Even Employee's witness, Lovett, testified that while she could have read Talley's messages, she chose not to. I do not find Employee credible when he insisted that he had to read parts of Talley's text messages to confirm that they had fully transferred. I find that the best person to confirm that all the data had been transferred would have been Talley herself, as she is the authorized user of the cellphones and would logically be more familiar with its contents than Employee.

Lastly, I find Employee's argument that there can be no reasonable expectation of privacy when using government-issued devices to be misguided. While data is indeed shared between fellow government employees, it is done so only for official business and limited to those with a need to know the said data.[2] I therefore find that Employee failed to protect the confidentiality of Talley's messages when he read them and then confronted Tonjes with the information he improperly obtained. Based on a preponderance of the evidence, I find that Employee neglected his duty to protect the confidentiality of government data and this failure amounted to misconduct prejudicial to the District. Accordingly, I find that Employee was guilty of all charges and specifications leveled by Agency.

If so, whether the penalty of termination was appropriate under the circumstances.

Employee argues that a proper analysis of the *Douglas* Factors would preclude termination as an appropriate penalty.[3] The D.C. Court of Appeals has made clear that a D.C. agency must

[2] Government data including those pertaining to national security has always been accorded the highest possible privacy protections by Congress and the courts. *See* 2021 Washington DC Legislative Resolution No. 996, Washington DC Council Period 24; *Grumman Aircraft Engineering Corp. v. Renegotiation Bd.*, 425 F.2d 578 (1970).

[3] In *Douglas v. Veterans Administration*, 5 M.S.P.R. 280, 305-306 (1981), the Merit Systems Protection Board, this Office's federal counterpart, set forth "a number of factors that are relevant for consideration in determining the appropriateness of a penalty." Although not an exhaustive list, the factors are as follows:

take into consideration the so-called "*Douglas* Factors" when making a disciplinary determination.[4] In *Douglas v. Veterans Administration,* the Merit Systems Protection Board ("MSPB"), in the context of federal employment, ruled that an agency must consider specific mitigating and aggravating factors in determining an appropriate penalty. The D.C. Court of Appeals in *Colbert* emphasizes the importance of responsibly balancing the relevant factors in each individual case. In its evaluation of the dismissal of a D.C. Department of Public Works employee and subsequent proceedings, the Appellate Court further explained that an agency must consider the *Douglas* Factors at the onset of termination and in consideration of pretermination protections.[5] The agency must provide evidence of the *Douglas* Factors in advance of termination to preserve the procedural protections of due process.

In this matter, Agency addressed the *Douglas* Factors in its Advance Written Notice of Proposed Removal on June 7, 2020.[6] It discussed *Douglas* Factors 1, 2, 5, 6, 7, 8, 9, 10, 11 and 12 and only found *Douglas* Factors 3 and 4 as mitigating. Essentially, Agency states that Employee's

> 1) The nature and seriousness of the offense, and its relation to the employee's duties, including whether the offense was intentional or technical or inadvertent, or was committed intentionally or maliciously or for gain, or was frequently repeated;
>
> 2) the employee's job level and type of employment, including supervisory or fiduciary role, contacts with the public, and prominence of the position;
>
> 3) the employee's past disciplinary record;
>
> 4) the employee's past work record, including length of service, performance on the job, ability to get along with fellow workers, and dependability;
>
> 5) the effect of the offense upon the employee's ability to perform at a satisfactory level and its effect upon supervisors' confidence in the employee's ability to perform assigned duties;
>
> 6) consistency of the penalty with those imposed upon other employees for the same or similar offenses;
>
> 7) consistency of the penalty with any applicable agency table of penalties;
>
> 8) the notoriety of the offense or its impact upon the reputation of the agency;
>
> 9) the clarity with which the employee was on notice of any rules that where violated in committing the offense, or had been warned about the conduct in question;
>
> 10) potential for the employee's rehabilitation;
>
> 11) mitigating circumstances surrounding the offense such as unusual job tensions, personality problems, mental impairment, harassment, or bad faith, malice or provocation on the part of others involved in the matter; and
>
> 12) the adequacy and effectiveness of alternative sanctions to deter such conduct in the future by the employee or others.

[4] *D.C. Department of Public Works v. Colbert*, 874 A.2d 353 (D.C. 2005).

[5] *Colbert* at 359.

[6] Agency Exhibit Tab 2.

failure to safeguard confidential/sensitive information that he encountered in his position as an IT Specialist had made Agency lose confidence in Employee.

Employee argues that Agency's *Douglas* Factor analysis is flawed in that Agency has failed to prove that his awareness of the text was intentional, technical, inadvertent, or committed maliciously or for gain, as he discovered the text through his normal course of work. Employee's other arguments regarding Agency's *Douglas* Factor analysis are premised on his disagreement with the way Agency did its analysis and the weight it placed on each factor. However, while there is a requirement that Agency perform a *Douglas* Factor analysis in deciding Employee's penalty, I find that there is no requirement that Agency perform such an analysis to Employee's satisfaction.[7]

As discussed above, I find that all the charges should be upheld. In determining the appropriateness of an agency's penalty, OEA has consistently relied on *Stokes v. District of Columbia*, 502 A.2d 1006 (D.C. 1985). According to the Court in *Stokes*, OEA must determine whether the penalty was within the range allowed by law, regulation, and any applicable Table of Penalties; whether the penalty is based on a consideration of the relevant factors, and whether there is a clear error of judgment by agency.

Chapter 16 of the DPM and the D.C. Municipal Regulations("DCMR") outlines the Table of Illustrative Actions ("TIA") for various causes of adverse actions taken against District government employees. DCMR § 6-B1607.2(a)(10) Conduct Prejudicial to the District provides that the penalty for a first offense of "unauthorized disclosure or use of (or failure to safeguard) information protected by statute or regulation or other official, sensitive or confidential information ranges from counseling to removal. The penalty for the first offense for DCMR § 6-B1607.2(e) Neglect of Duty: Failing to carry out official duties or responsibilities as would be expected of a reasonable individual in the same position; careless work habits" ranges from counseling up to removal. In short, even if Employee was guilty of only one of the charges or specifications, the allowable penalty for a first offense includes removal.

Based on the foregoing, I do not find that Agency exceeded the limits of reasonableness with the penalty imposed against Employee. Accordingly, in light of the testimony and evidence presented, I find that Agency's penalty of termination was appropriate for the sustained charges of prejudicial conduct to the District and neglect of duty.

ORDER

Accordingly, it is hereby **ORDERED** that Agency's termination of Employee is UPHELD.

FOR THE OFFICE:

Joseph Lim
Joseph E. Lim, Esq.
Senior Administration Judge

[7] *District of Columbia Metropolitan Police Dept. v. District of Columbia Office of Employee Appeals*, 88 A.3d 724 (April 10, 2014) the D.C. Court of Appeals has held that an agency is not required to articulate its Douglas analysis regarding factors that assist it in determining appropriateness of sanction, before terminating employee.