

**LAI-ON-THE-TABLE**

Submitted by: Assembly Chair Constant and Vice  
Chair Zaletel  
Prepared by: Assembly Counsel's Office  
For reading: September 12, 2023

**ANCHORAGE, ALASKA**  
**AR No. 2023-\_\_\_\_\_**

**RESOLUTION OF THE ANCHORAGE ASSEMBLY APPROVING THE USE OF  
SUBPOENAS TO COMPEL TESTIMONY AND DOCUMENT PRODUCTION  
PURSUANT TO ANCHORAGE MUNICIPAL CODE SECTION 2.30.085 AND  
AUTHORIZING LITIGATION TO ENFORCE COMPLIANCE WITH THOSE  
LEGISLATIVE SUBPOENAS.**

---

**WHEREAS**, Anchorage Municipal Code section 2.30.085, *Subpoena powers*, authorizes the Assembly Chair, with the approval of a majority of the Assembly, to compel by subpoena the “testimony of a person whom the assembly reasonably believes may be able to give information relating to a matter involving municipal funds and policy being considered” and to “produce documents, papers or objects which the assembly reasonably believes may relate to the matter under consideration”; and

**WHEREAS**, the Municipal Ombudsman has recently investigated the facts and circumstances surrounding use of an IT Department internal policy statement in an election complaint filed by the Mayor’s former Chief of Staff, Ms. Sami Graham; and

**WHEREAS**, the Municipal Ombudsman found that the current IT Director, Mr. Marc Dahl, initiated and directed the revision and posting of the OIT USB policy to provide support for Ms. Graham’s challenge of the April 4, 2023 Municipal election, that Mr. Dahl had communicated directly with Ms. Graham to provide her a copy of the policy statement, and that Ms. Graham cited policy statement in her complaint; and

**WHEREAS**, the Municipal Charter vests the responsibility for administration and adjudication of elections in the Assembly as the legislative branch of the Municipal Government; and

**WHEREAS**, the Assembly is bound by duty, not only to their office, but to the people of the Municipality of Anchorage, to investigate any attempt to subvert the electoral process and to propose legislative solutions to ensure the security of our elections; and

**WHEREAS**, the 2024 Regular Election process will formally begin with posting of the notice of vacancies on January 8, 2024; and

**WHEREAS**, any amendment to Title 28 of the Anchorage Municipal Code must be introduced by the December 5, 2023 regular meeting of the Assembly in order to be enacted by the Assembly before the 2024 Regular Election; and

**WHEREAS**, any investigation by the Assembly into these matter will need to

1 conclude before the November 22, 2023 Agenda deadline, to give the body any  
2 meaningful opportunity to craft appropriate legislation to introduce at the December  
3 5, 2023 regular meeting; and  
4

5 **WHEREAS**, the Assembly Chair and Vice Chair have repeatedly requested  
6 information from the Administration regarding the facts and circumstances that led  
7 to the publication of the ITD Policy Statement and its role in the complaint filed by  
8 Ms. Graham; and  
9

10 **WHEREAS**, very limited requested information has been provided after reasonable  
11 and diligent efforts to obtain with multiple requests to the Administration staff; and  
12

13 **WHEREAS**, the Mayor has declined to take any action regarding these allegations  
14 and publicly expressed that he does not “see any evidence that Mr. Dahl conducted  
15 any illegal behavior” and that it is merely “the timing in which the events occurred,  
16 and the lack of process followed that is in question”; and  
17

18 **WHEREAS**, in investigating this matter the Ombudsman explicitly found that “the  
19 timeline, and Dahl’s email to Graham demonstrate that Dahl was directing the  
20 development and posting of the policy to provide support for the impending election  
21 challenge”; and  
22

23 **WHEREAS**, the Chair of the Assembly now requests authorization of the Assembly,  
24 per AMC section 2.30.085, to issue subpoenas as the next step to obtain requested  
25 information;  
26

27 **NOW, THEREFORE BE IT RESOLVED THAT THE ANCHORAGE ASSEMBLY:**  
28

29 **Section 1.** Does hereby, pursuant to AMC section 2.30.085, authorize the Chair  
30 of the Assembly to compel by subpoena the attendance of persons to provide  
31 testimony or produce documents at a time and place specified by the Chair, as  
32 described below:  
33

- 34 A. Any documents relevant or related to the election complaints filed by  
35 Ms. Graham on April 11, 2023, and/or presented by Ms. Sami Graham  
36 to the Election Commission at the April 20, 2023 public session of  
37 canvass;  
38
- 39 B. Any documents relevant or related to the creation, publication, or  
40 distribution of the Department of Information Technology Policy  
41 Statement Concerning Access To or Connection of Removeable  
42 Storage (USB) Devices, including but not limited to copies of any  
43 internal reports or investigations conducted by the Administration into  
44 the matter;  
45
- 46 C. Any witness who communicated with Ms. Graham, or otherwise  
47 possessing information relevant or related to the election complaint  
48 filed by Ms. Sami Graham challenging the results of the 2023 Regular  
49 Election or the creation;  
50

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39

D. Any record of communication or correspondence to, from, between, or among any current or former public official, including but not limited to the Mayor, the Municipal Manager, the Chief of Staff, IT Director any of their deputies, or contract employees, discussing complaints or allegations of misconduct in either the 2022 or 2023 Regular Election; and

E. Records of any communications or correspondence to, from, between, or among any current or former public official, including but not limited to the Mayor, the Municipal Manager, the Chief of Staff, any of their deputies, contract employees or any other municipal employee and Ms. Graham.

**Section 2.** Authorizes the Assembly Counsel’s Office to initiate and expedite litigation, on behalf and in the name of the Anchorage Municipal Assembly, appropriate to compel the attendance of any witness or the release of the records in question and enforce compliance with the Chair’s subpoenas, or other matters relevant to the Assembly’s investigation. Assembly Counsel may, for the Anchorage Municipal Assembly, file an original action, intervene or otherwise seek to participate in any pending action, and request expedited consideration, either as Counsel deems most advisable, or through contracted outside counsel, and after conferring with the Assembly Chair and Vice Chair.

**Section 3.** This resolution shall be effective immediately upon passage and approval by the Assembly.

PASSED AND APPROVED by the Anchorage Assembly this \_\_\_\_\_ day of \_\_\_\_\_, 2023.

\_\_\_\_\_  
Chair of the Assembly

ATTEST:

\_\_\_\_\_  
Municipal Clerk



## MUNICIPALITY OF ANCHORAGE

### Assembly Information Memorandum

No. AIM \_\_\_\_ - 2023

Meeting Date: September 12, 2023

1 **From:** ASSEMBLY CHAIR CONSTANT

2  
3 **Subject:** FACTS AND CIRCUMSTANCES SURROUNDING THE  
4 CREATION OF AN ITD POLICY STATEMENT REGARDING  
5 REMOVABLE STORAGE DEVICES AND ITS ROLE IN THE  
6 FILING OF AN ELECTION COMPLAINT IN THE 2023 REGULAR  
7 ELECTION.  
8

9 This information memorandum provides a record of the events that led to the  
10 creation, posting, and transmission of a policy statement regarding the use of USB  
11 devices in municipal equipment, and the manner in which that internal policy  
12 statement was used to challenge the results of the 2023 regular election.  
13

14 On January 10, 2023, the Chief Information Security Officer, Mark Merchant sent  
15 an email to the IT Director, Marc Dahl, Cc'ing Anna Plant with the subject "FW:  
16 Policy – 28-10." (Attachment A). The email provided two Policy and Procedure  
17 documents: one titled, "PP 28-7 Password Management 101521" and second  
18 titled, "PP 28-10 Protection of Personal or Confidential Information 091421 –  
19 Final.doc." (Tabs A.1-2). It is unclear why this email was sent from Mr. Merchant  
20 to Mr. Dahl, although the body of the email stated, "These are the two that we were  
21 working on", implying that there had been some discussion prior to this email being  
22 sent. The Administration initially asserted that the entire body of this email, as well  
23 as the entirety of the of one of the attached documents, PP 28-10, were privileged  
24 from disclosure pursuant to the deliberative-process privilege, but it has  
25 subsequently withdrawn that assertion of privilege at the request of the Assembly  
26 Leadership.  
27

28 On January 18, 2023, Mark Merchant sent an email to Marc Dahl with the subject  
29 "Draft Round 2" which included an attachment titled, "PP\_28-41\_Internet and  
30 System Connectivity01183.docxdoc." (Attachment B). The text of the email states  
31 simply "FYI. Please review and add content." Although the subject indicates that  
32 the email is forwarded from an original sender, there is no historical email thread  
33 contained in the body of the email, making it unclear what the provenance of the  
34 original email is. The Administration initially asserted that the entire body of this  
35 email, as well as the entirety of the attached document was privileged from  
36 disclosure pursuant to the deliberative-process privilege, but it has subsequently  
37 withdrawn that assertion of privilege at the request of the Assembly Leadership.  
38

39 On April 6, 2023, Ms. Sami Graham, an election observer affiliated with John



1 Trueblood, a candidate for a seat in District 1 of the Anchorage Assembly, filed a  
2 Complaint Form regarding the Municipal election. (Attachment C). The complaint  
3 alleged that current practices it was “completely possible” that the thumb drive  
4 used to transfer data from Dominion equipment to an MOA computer could be  
5 “depositing or altering data, intentionally or unintentionally, [and] not simply  
6 retrieving data.” The complaint specifically requested that “anytime any device is  
7 connected to the Dominion machine a qualified and mutually agreed upon member  
8 of M.O.A. IT dept. be present to supervise”. In addition to requesting the election  
9 officials change their process by which it tabulated votes in the middle of an  
10 election, this complaint failed to cite to any factual basis for this concern.

11  
12 On April 7, 2023, MOA Election Administrator Jamie Heinz responded to Ms.  
13 Graham’s complaint (Attachment D). Ms. Heinz noted that the election thumb  
14 drives: (1) Are stored in a wall safe inside a locked room which requires a code  
15 and thumb print to open; (2) Are encrypted and reformatted each year according  
16 to Municipal IT practices; and (3) Require a password to receive any download of  
17 election results. Ms. Heinz determined that there was no “misconduct,” as Ms.  
18 Graham did not allege any failure comply with any law or illegal election practice.  
19 Ms. Heinz informed Ms. Graham that the complaint would be treated as a  
20 suggestion related to administrative or management concerns.

21  
22 On April 11, 2023, a significant amount of email traffic occurred (Attachment E):

23  
24 At 8:45 am, Mark Merchant sent an email to Marc Dahl forwarding his earlier  
25 January 18<sup>th</sup> email with the text “FYI. Here was the latest draft that we did back in  
26 January.” (Tab E.1. This actual email was not provided to the Assembly, but can  
27 be found in the email thread contained in the 9:30am email sent by Mr. Merchant).  
28 It is unclear what prompted this email.

29  
30 At 8:59 am, Mr. Dahl replied with the text “I don’t see any reference to thumb  
31 drives and data exchange on critical infrastructure.” (Tab E.1)

32  
33 At 9:30 am, Mr. Merchant replied to Mr. Dahl stating “This is all that’s on  
34 there...” (Tab E.1). followed by an excerpt from the draft PP 28-41 which was  
35 originally in the January 18, 2023 email Mr. Merchant sent to Mr. Dahl. The  
36 Administration initially asserted that the entire body of this email, as well as the two  
37 previous emails which are visible within the thread of this email, were privileged  
38 from disclosure pursuant to the deliberative-process privilege, but it has  
39 subsequently withdrawn that assertion of privilege at the request of the Assembly  
40 Leadership.

41  
42 At 10:09 am, Mr. Dahl, replied to Mr. Merchant requesting he “[p]lease update  
43 to be specific on who performs the scan. For critical infrastructure the scanning  
44 needs to be limited to Security, Infrastructure or Network team or pre-registered  
45 technically capable delegate.” (Tab E.2). The Administration initially asserted that  
46 the entire body of this email was privileged from disclosure pursuant to the  
47 deliberative-process privilege, but it has subsequently withdrawn that assertion of  
48 privilege at the request of the Assembly Leadership.

49  
50 At 10:14 Mr. Merchant replies to Mr. Dahl, saying “Will do....I’ll work on it.” A

1 portion of this email is redacted as containing personal information not subject to  
2 disclosure as a public record. (Tab E.3). The Administration initially asserted that  
3 the entire body of this email was privileged from disclosure pursuant to the  
4 deliberative-process privilege, but it has subsequently withdrawn that assertion of  
5 privilege at the request of the Assembly Leadership.  
6

7 At 10:42 am, Mr. Dahl, sent an email to Mr. Merchant saying “Come back with  
8 what you recommend. This is a conversation not a dictate.” (Tab E.4). The  
9 Administration initially asserted that the entire body of this email was privileged  
10 from disclosure pursuant to the deliberative-process privilege, but it has  
11 subsequently withdrawn that assertion of privilege at the request of the Assembly  
12 Leadership.  
13

14 At 12:16 pm Mr. Merchant sent an email Mr. Dahl with the same subject line  
15 with the text “Getting close...” in the body of the email followed by the language  
16 the comprises the USB policy at issue. (Tab E.5).  
17

18 At 1:20 pm Mr. Merchant emailed Heather Holland requesting the creation of a  
19 new link called “ITD Policy statements”. (Tab E.6). Mr. Merchant emphasizes that  
20 “This is one Marc would like to put up as soon as possible.” It is not clear how the  
21 urgency of this document being posted was communicated to Mr. Merchant.  
22

23 At 1:31 pm, Ms. Holland responded to Mr. Merchant informing him the page  
24 has been created and providing him a link to it. (Tab E.7).  
25

26 At 2:00 pm, Mr. Dahl sent an email to himself with the link provided by Ms.  
27 Holland, and the text of an ITD Policy Statement titled “Access to or connection of  
28 Removeable Storage (USB) devices.” (Tab E.9).  
29

30 At 2:37 pm, Mr. Dahl sent an email to alaskansam@yahoo.com with the text,  
31 “Published on the internal IT Security web page,” followed by the link provided by  
32 Ms. Holland and the text of an ITD Policy Statement titled “Access to or connection  
33 of Removeable Storage (USB) devices.” It is unclear whether anyone else was  
34 notified of the existence of this new page on the sharepoint site. (Tab E.10).  
35

36 At or about 3:47 pm, Ms. Graham filed a second complaint “[a]s an appeal to  
37 comments received on Apr. 6 (*sic*) 2023, from Jamie Heinz.” (Attachment F). This  
38 complaint explicitly references the MOA ITD practices, according to MOA ITD  
39 policy statement, stating.

40 “Personnel must not insert an unauthorized USB device into any  
41 piece of M.O.A. owned equipment without authorization from the  
42 Information Technology Dept. (ITD) and only after the USB devices  
43 have been scanned for malware by ITD. All insertions into MOA  
44 Critical Infrastructure technology must also be approved and/or  
45 observed by ITD management and must follow ITD change  
46 management process and procedures regarding patch management  
47 & malware remediation.’ We believe the clerk’s current practices in  
48 relation to Thumb drive statement (*sic*) is a clear violation of the MOA  
49 ITD USB policy statement.”

50 The complaint form required a statement of how the concern, if true, would change

1 the outcome of the election. In response Ms. Graham reasserted that “It is  
2 completely possible that the USB device is depositing or altering data, intentionally  
3 or unintentionally, not simply retrieving data, thereby nullifying the results of the  
4 election.” Again, Ms. Graham failed to provide any factual basis for this purported  
5 possibility.

6  
7 On April 14, 2023 at 11:31am, Mr. Dahl sent an email to alaskansam@yahoo.com  
8 with the text “See this proposed code update being introduced at the next  
9 assembly.” Followed by what appears to be the entry for AO 2023-45 copied from  
10 Assembly’s Agenda for its special meeting on April 18, 2023. (Attachment G). Later  
11 that day, Ms. Graham filed a third complaint form with the Clerk’s Office, alleging  
12 that “[t]he Assembly item 5.A. No 2023-45, written by Christopher Constant - a  
13 candidate in the current election - is a direct response to the appeal dated Apr. 11.  
14 It changes the processes and procedures of an election during the middle of an  
15 election.” (Attachment I).

16  
17 On April 16, 2023, at 3:39 pm, Ms. Heinz responded to Ms. Graham’s renewed  
18 complaint via email sent to alaskansam@yahoo.com , informing her that the  
19 Ordinance at issue was introduced at the April 7th Special Meeting and attaching  
20 emails stating the deadlines for submission for that meeting’s was noon on  
21 Wednesday, April 5th as well as an email from the Municipal Clerk’s office which  
22 had been sent out at 10:57 a.m. on Thursday, April 6th, and contained the entire  
23 packet of materials for the April 7th Special Meeting. (Attachment J). At 4:16 pm  
24 Ms. Graham sent an email to Ms. Heinz from the email account  
25 alaskansam@yahoo.com withdrawing the April 14 complaint. (Attachment K).

26  
27 On April 20, 2023, Ms. Graham appeared at the public session of canvass to  
28 present her complaint in person to the Election Commission as Agenda Item 5.C.a.  
29 “Failure to Comply with Law or Alleged Illegal Election Practices re MOA ITD USB  
30 Policy Statement.” Her public testimony focused on the transfer of data via USB  
31 devices without the involvement of the IT Department, although she did voice the  
32 same concerns regarding AO 2023-45 she expressed in her April 14, 2023  
33 complaint. Although Ms. Graham declined to state a specific remedy she desired  
34 from the Commission, the only relief that it could feasibly grant her would be to  
35 report to the Assembly a failure to comply with the provisions of law or illegal  
36 election practices sufficient to change the outcome of the election under AMC  
37 28.85.040, and to recommend the entire election be declared invalid. The  
38 Commission ultimately dismissed her complaint. (Attachment L. Recording  
39 available here: [https://www.youtube.com/watch?v=x14b96\\_ZKCs](https://www.youtube.com/watch?v=x14b96_ZKCs)).

40  
41 On April 26, 2023, the Municipal Ombudsman received complaint from a  
42 constituent questioning how the ITD Policy Statement relied upon in Ms. Graham’s  
43 election complaint came into being and how it came into her possession.

44  
45 On July 5, 2023, The Assembly Leadership sent a letter to the Bronson  
46 Administration, announcing a work session and inviting their participation  
47 (Attachment M). Additionally, the Leadership stated multiple questions they would  
48 seek to address as part of their inquiry into this matter.

49  
50 On July 10, 2023, the Assembly Chair submitted a public records request to the

1 Department of Law, requesting, among other things, communications between the  
2 IT Department and Ms. Sami Graham (Attachment N). The records provided in  
3 response to this request make up the bulk of the substantive information contained  
4 in this AIM.

5  
6 On July 21, 2023 the Assembly held a worksession to discuss the election  
7 complaint submitted by Ms. Graham on April 11, 2023 and the role Mr. Dahl's "ITD  
8 Policy Statement" played in that complaint. The Administration had provided many  
9 of the documents requested by the Chair in his July 10<sup>th</sup> email in advance of the  
10 worksession, and these documents were made available to the members. As  
11 noted in this memorandum, several documents were, at the time, redacted to  
12 preserve potentially privileged information pursuant to the deliberative-process  
13 privilege. The Administration was represented by Municipal Manager, the Chief of  
14 Staff and the Department of Law at this worksession. The Administration declined  
15 to take any position on the evidence presented as the Ombudsman had not  
16 completed his investigation at that point.

17  
18 On July 25, 2023, the Ombudsman submitted his initial findings to the  
19 Administration for comment.

20  
21 On August 17, 2023, the Administration provided the Ombudsman with their written  
22 response to his initial findings. The Ombudsman incorporated the substance of  
23 their responses into the body of the final report, and, additionally, their written  
24 memorandum in its original form was attached as appendix. In his final published  
25 report, the Ombudsman recommended, among other things, that the  
26 Administration terminate Mr. Dahl's employment, finding that he had "damaged the  
27 reputation of the Municipality's Office of Information technology and [had]  
28 undermined the trust of other Municipal departments, agencies, and employees...  
29 necessary for the department to accomplish its mission." The Administration  
30 declined to comment on either this recommendation or finding. (Attachment O).

31  
32 On August 18, 2023, Assembly Leadership sent a letter to the Administration  
33 disputing their assertion of the deliberative-process privilege in certain  
34 communications it had provided in response to the Chair's July 10<sup>th</sup> records  
35 request. Assembly Leadership closed by requesting the release of the unredacted  
36 emails sent between Mr. Dahl and Mr. Merchant that preceded the creation of the  
37 ITD Policy Statement. (Attachment P).

38  
39 On September 5, 2023, Assembly Leadership sent the Administration a letter  
40 requesting "[r]ecords of any communications to, from, or between current and  
41 former employees of your office discussing complaints or allegations of misconduct  
42 in either the 2022 or 2023 Regular Election" and "[r]ecords of any communications  
43 to, from, or between current or former employees of your office or any other current  
44 or former municipal employee and Ms. Sami Graham."

45  
46 On September 8, 2023, the Assembly held a second worksession at which the  
47 Ombudsman presented his report. The Administration failed to send a  
48 representative or provide any of the documents requested in either of the  
49 Assembly Leadership's previous requests. That evening Mayor Bronson provided  
50 his first public comments on the alleged actions of Mr. Dahl and Ms. Graham

1 stating that he did not “see any evidence that Mr. Dahl conducted any illegal  
2 behavior” and that it is merely “the timing in which the events occurred, and the  
3 lack of process followed that is in question.”  
4

5 On September 11, 2023, the Administration provided the previously redacted  
6 emails the Assembly Chair initially requested on July 10<sup>th</sup> and for which the  
7 Assembly Leadership renewed this request on August 18, 2023.  
8

9 As of the submission of this memorandum, Mr. Dahl is still employed as the  
10 Director of the Municipal Information Technology Department.  
11

12 Prepared by: Assembly Counsel’s Office  
13

14 Respectfully submitted: Christopher Constant, Assembly Chair  
15 District 1, North Anchorage  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35

## Table of Attachments

---

1		
2		
3	Attachment A - Jan. 10 Email from Mr. Merchant to Mr. Dahl.....	1
4	Attachment B - Jan. 18 Email from Mr. Merchant to Mr. Dahl .....	13
5	Attachment C - Apr. 6 Complaint from Ms. Graham.....	18
6	Attachment D - Clerk response to Apr. 6 Complaint.....	19
7	Attachment E - Apr. 11 ITD Emails.....	20
8	Attachment F - Apr. 11 Ms. Graham Appeal.....	43
9	Attachment G - Apr. 14 Email from Mr. Dahl to alaskansam@yahoo.com.....	45
10	Attachment H - Apr. 14 Email from Mr. Dahl to Muni Attorney.....	46
11	Attachment I - Apr. 14 Ms. Graham Appeal.....	48
12	Attachment J - Clerk response to Apr. 14 Complaint.....	50
13	Attachment K - Apr. 16 Email from Ms. Graham.....	53
14	Attachment L - Election Commission Agenda.....	55
15	Attachment M - Letter to Mayor Bronson.....	56
16	Attachment N - Chair's records request.....	60
17	Attachment O - Ombudsman's Report.....	61
18	Attachment P - Leadership August 18, 2023 Letter to Mayor.....	71
19	Attachment Q - Leadership Sep. 5, 2023 Letter to Mayor.....	76
20	Attachment R - Sep. 8, 2023 KTUU article quoting Mayor.....	79
21		

Attachment A

**Date :** 1/10/2023 1:05:09 PM  
**From :** "Merchant, Mark A."  
**To :** "Dahl, Marc"  
**Cc :** "Plant, Anna L."  
**Subject :** FW: Policy - 28-10  
**Attachment :** PP 28-7 Password Management 101521.doc;PP 28-10 Protection of Personal or Confidential Information 091421 - Final.doc;image001.jpg;

Hey Marc,

These are the two that we were working on. The Password Mgmt. (28-7) was approved but the Protection of PII (28-10) was waiting for Amy to review prior to the Mayor signing it. Maybe we can just get the Mayor to sign it now. It has already been approved through Legal and OMB.

Thanks.

*Thank you for helping us to protect our personal information.*

***Mark Merchant, CISSP, GCEA, LASO***

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Merchant, Mark A.  
**Sent:** Monday, October 25, 2021 9:32 AM  
**To:** Dahl, Marc <marcus.dahl@anchorageak.gov>  
**Subject:** FW: Policy - 28-10

Christine is reviewing these and will forward them to Amy and then get the Mayor to sign them.

*Thank you for helping us to protect our personal information.*

***Mark Merchant, CISSP, GCEA, LASO***

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Merchant, Mark A.  
**Sent:** Monday, October 25, 2021 9:24 AM

## Attachment A

**To:** Chesnut, Christine L. <[christine.chesnut@anchorageak.gov](mailto:christine.chesnut@anchorageak.gov)>

**Subject:** RE: Policy - 28-10

Also,

We updated the MOA Password Policy to modify the password change frequency from 90 days to 365. (7.e.i.B) for standard MOA employees... Can we please get this signed at the same time?

- (B) Ensure that password history is enabled, which will prevent the reuse of any of the previous ten (10) passwords; that password expiration does not exceed 365 days for standard user accounts and 90 days for accounts with Admin (ADM) or elevated privileges.

*Thank you for helping us to protect our personal information.*

**Mark Merchant**, CISSP, GCEA, LASO

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Chesnut, Christine L. <[christine.chesnut@anchorageak.gov](mailto:christine.chesnut@anchorageak.gov)>

**Sent:** Monday, October 25, 2021 8:55 AM

**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>

**Subject:** RE: Policy - 28-10

Ok, so the Director doesn't do anything say in an IT system to encrypt this, it is part of the normal process, but the Director is responsible to ensure that the information stays encrypted?

This is under the procedure section, so I was looking for the process a Director must follow. It sounds like they don't actually have to do anything, just adhere to the fact that it must stay encrypted.

Is that correct?

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>

**Sent:** Monday, October 25, 2021 8:50 AM

**To:** Chesnut, Christine L. <[christine.chesnut@anchorageak.gov](mailto:christine.chesnut@anchorageak.gov)>

**Subject:** RE: Policy - 28-10

Thanks Christine!

So any Director that is in charge of data like Public Health Information or Criminal Justice Information will know that this type of "data in transit" or "data at rest" must be encrypted per Federal Law. As the Director, they should know where this



type of data exists in their environment and should make sure that IT is encrypting it so they are in compliance.

Does that help?

*Thank you for helping us to protect our personal information.*

**Mark Merchant, CISSP, GCFA, LASO**

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Chesnut, Christine L. <[christine.chesnut@anchorageak.gov](mailto:christine.chesnut@anchorageak.gov)>

**Sent:** Monday, October 25, 2021 8:43 AM

**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>

**Subject:** FW: Policy - 28-10

Hi Mark,

I have one question prior to moving this forward.

Section 7.d. How will a Director know how to implement encryption?

Apologies for the delay. Once this question is resolved, Leilah will then package this up for the Muni Mgr, then Mayor's signature.

Thanks!

---

**From:** Lawyer, Leilah I. <[leilah.lawyer@anchorageak.gov](mailto:leilah.lawyer@anchorageak.gov)>

**Sent:** Wednesday, October 13, 2021 9:51 AM

**To:** Chesnut, Christine L. <[christine.chesnut@anchorageak.gov](mailto:christine.chesnut@anchorageak.gov)>

**Subject:** RE: Policy - 28-10

Hi Christine,

Sorry to bother. Have you had a chance to review this P&P? Mark Merchant pinged me this morning asking for the status of this P&P (I honestly forgot about it). Please let me know if you need anything. Thanks!

**Leilah Lawyer**

Office of Management and Budget

Administrative Officer

Ext. 4496

---

**From:** Lawyer, Leilah I.

**Sent:** Monday, September 20, 2021 2:21 PM

**To:** Chesnut, Christine L. <[christine.chesnut@anchorageak.gov](mailto:christine.chesnut@anchorageak.gov)>

**Subject:** FW: Policy - 28-10

Hi Christine,

I have logged this, added the definitions to our master definitions list, formatted it, and I also added section #9 Annual Review Date/Lead Review Agency.

The department's version that they sent me ends with "091421 – Final". The version that I updated ends with "OMB".

Please let me know when you have had a chance to review. I will then send it to Karl. Thank you!

**Leilah Lawyer**  
Office of Management and Budget  
Administrative Officer  
Ext. 4496

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Monday, September 20, 2021 10:20 AM  
**To:** Lawyer, Leilah I. <[leilah.lawyer@anchorageak.gov](mailto:leilah.lawyer@anchorageak.gov)>  
**Cc:** Ennis, Deitra L. <[deitra.ennis@anchorageak.gov](mailto:deitra.ennis@anchorageak.gov)>; Sherwood, Todd K. <[todd.sherwood@anchorageak.gov](mailto:todd.sherwood@anchorageak.gov)>; Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** FW: Policy - 28-10

Good morning Leilah,

I found out Darlene Williams is no longer working for OMB and your name came up, so I am hoping this is the right place. ☐

The attached enterprise security policy has been reviewed by Legal, the IRT and multiple Department Directors and we wanted to get final OMB approval and formatting prior to the Mayor's signature.

Please let me know if you have any questions or concerns.

*Thank you for helping us to protect our personal information.*

**Mark Merchant, CISSP, GCFA, LASO**  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Sherwood, Todd K. <[todd.sherwood@anchorageak.gov](mailto:todd.sherwood@anchorageak.gov)>  
**Sent:** Thursday, September 9, 2021 1:27 PM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>; Ennis, Deitra L. <[deitra.ennis@anchorageak.gov](mailto:deitra.ennis@anchorageak.gov)>; Plant, Anna L. <[anna.plant@anchorageak.gov](mailto:anna.plant@anchorageak.gov)>; Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** RE: Policy - 28-10

Looks ok to me.



**Todd Sherwood**

*Assistant Municipal Attorney*

Municipality of Anchorage

632 W.6<sup>th</sup> Avenue, Suite 730 Anchorage, Alaska 99501

(907) 343-4545

[todd.sherwood@anchorageak.gov](mailto:todd.sherwood@anchorageak.gov)

[www.muni.org/Departments/Legal/](http://www.muni.org/Departments/Legal/)

This e-mail transmission and any documents accompanying it may contain confidential information that is protected by attorney-client privilege or other grounds for confidentiality or nondisclosure. If you are not the intended recipient of the transmitted information, you are hereby notified that disclosing, copying, distributing, or taking action in reliance on the contents of the information is prohibited. If you have received this transmission in error, please notify our office by calling (907) 343-4545 or by responding to this email, and then promptly delete the information.

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>

**Sent:** Thursday, September 09, 2021 12:31 PM

**To:** Ennis, Deitra L. <[deitra.ennis@anchorageak.gov](mailto:deitra.ennis@anchorageak.gov)>; Sherwood, Todd K.

<[todd.sherwood@anchorageak.gov](mailto:todd.sherwood@anchorageak.gov)>; Plant, Anna L. <[anna.plant@anchorageak.gov](mailto:anna.plant@anchorageak.gov)>;

Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>

**Subject:** Policy - 28-10

**Importance:** High

Ok, this policy has been updated after our meeting today. Please take a look and let me know if I captured and entered everything correctly. I highlighted all the changes that we made to make for a quick review.

Thanks again everyone!

*Thank you for helping us to protect our personal information.*

**Mark Merchant**, CISSP, GCFA, LASO

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917


C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**MOA Internal Only**

**Warning: The information within this email and any attached document is classified FOR OFFICIAL INTERNAL USE ONLY (Confidential – MOA Internal Only).** It contains information that may be exempt from public release under the Alaska Public Records Exception (AS 40.25.120 (a) (10)). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with MOA policy relating to confidential information and is not to be released to the public, or other personnel who do not have a valid "need-to-know", without prior written authorization from the CIO or CISO. **No portion of this email or attached documents shall be**

**furnished to the media, either in written or verbal form.**

 <b>MUNICIPALITY OF ANCHORAGE O P E R A T I N G P O L I C Y / P R O C E D U R E</b>	P&P No. <b>28-7</b>	Page 1 of 3
	Effective Date: <b>August 1, 2018</b>	
Subject:  <b>Password Management</b>	Supersedes No. <b>Updated</b>	Dated:
	Approved by:	

1. PURPOSE

To ensure that proper password controls are applied to all Municipality of Anchorage (MOA) computer, network, and application accounts to meet or exceed the minimum regulatory compliance standards for data integrity and confidentiality.

2. POLICY

It is the policy of the Municipality to establish a baseline password requirement for all MOA owned computer systems and/or networked devices. Departments must meet or exceed this baseline policy.

3. ORGANIZATIONS AFFECTED

All Municipal agencies.

4. REFERENCES

National Institute for Standards and Technology Special P 800-63 Password Guidelines.

5. DEFINITIONS

- a. Data – numerical or other information represented in a form suitable for processing by computer.
- b. Encryption – A technical security control used to protect the confidentiality of an information asset.
- c. Standard User Account – Non-privileged accounts that do not have the ability to install applications, programs, or the ability to modify operating system configurations.
- d. Elevated or Admin (ADM) Accounts – Accounts with the ability to install applications or programs on desktops / servers and/or modify operating system configurations.

6. RESPONSIBILITIES

- a. The Chief Information Security Officer (CISO) shall be responsible for oversight of all MOA Information security.
- b. All Departmental IT staff shall configure and manage MOA systems to meet or exceed these password requirements.

7. PROCEDURE

- a. Strong Password Requirements
  - i. Personnel must set a password of sufficient length and complexity according to the following standards:

Subject: <b>Password Management</b>	P&P No. <b>28-7</b>	<b>Page 2 of 3</b>
----------------------------------------	------------------------	--------------------

- a. The password length must be 14 characters or more unless prohibited by application or system design;
  - b. The password must contain a combination of upper and lower case letters and include at least one numeric and/or special character (e.g., \$, (, %, @);
  - c. The password must not be a single word that would appear in a dictionary and must not be based on personal information (e.g., a pet name) or other identifiers (e.g., a social security number).
  - d. The password shall not be any of your previous 10 passwords.
- b. **Password Variability**
- When re-setting a password, personnel must use a new password that is substantially different from the old password. Personnel must not use passwords that are only incrementally different from the previous password (e.g., Thecowjumpedoverthemoon1, Thecowjumpedoverthemoon2, Thecowjumpedoverthemoon3.)
- c. **Application of Passwords**
- With the exception of public-access terminals or by management authorization, for example: servers, workstations, terminals and laptop computers, shall be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the system will be unattended.
- d. **Protections from Disclosure**
- i. Personnel must not record or store a password in any form (e.g., sticky note, notebook, electronic file) unless the password is protected by a technique (e.g., encrypted password storage application, sealed envelope in a limited-access safe, or other locked storage) and explicitly approved by IT Security via a Service Desk request. Passwords must not be inserted into electronic messages, or included in information transmitted by an electronic messaging system; the only exception is when the message is protected by an approved method or the password is a one-time use password.
  - ii. Personnel must not share a password or non-public account information assigned to them (Note: MOA technical personnel do not request passwords from personnel for any purpose).
  - iii. When a system, network, process, or application requires the use of a shared account or password, personnel must ensure that the number of individuals with the account information is limited to the minimum necessary for authorized purposes, and that the password is changed whenever there is a change in staff with knowledge of the account information.
  - iv. Personnel must immediately report any known or suspected compromise of a password to the MOA Security Office, in accordance with the MOA Incident Response Plan.


Subject: <b>Password Management</b>	P&P No. <b>28-7</b>	<b>Page 3 of 3</b>
----------------------------------------	------------------------	--------------------

- e. Proper Administration of Passwords
  - i. Personnel tasked with system administration responsibilities must
    - (A) Ensure that MOA systems, networks, and applications are configured to store passwords only when required and only in encrypted form.
    - (B) Ensure that password history is enabled, which will prevent the reuse of any of the previous ten (10) passwords; that password expiration does not exceed 365 days for standard user accounts and 90 days for accounts with Admin (ADM) or elevated privileges.
    - (C) Ensure that initial and reset passwords are set according to the password strength standards set forth in this policy, and that account users are required to change an initial or reset password upon logon. Personnel tasked with resetting passwords must ensure that any individual requesting a reset is positively identified and that the reset password is provided by an approved method.
    - (D) Ensure that passwords for service accounts are not provided to individuals without a legitimate requirement, are disabled when not in use, and are changed whenever there is a change in service personnel.
    - (E) Ensure that a mechanism is in place for each system, network, and application account with system-level privileges that allows the actions of an administrator to be uniquely associated with that individual.
    - (F) Not assign the same password to accounts with system-level privileges as is used for non-administrator accounts.
    - (G) Ensure that vendor-supplied default passwords for systems or applications are changed before the systems or applications are used for MOA purposes.
    - (H) Review users' access rights to systems at a minimum of once a quarter.

#### 8. REVIEW DATE/LEAD REVIEW AGENCY

The Office of Information Technology Department will review this document in October of each year for any needed revisions.



 <b>MUNICIPALITY OF ANCHORAGE O P E R A T I N G P O L I C Y / P R O C E D U R E</b>	P&P No. <b>28-10</b>	Page 1 of 2
	Effective Date: <b>September 1, 2021</b>	
Subject: <b>Protection of Personal or Confidential Information</b>	Supercedes No. <b>NEW</b>	Dated:
	Approved by:	

1. PURPOSE

To ensure appropriate safeguards are implemented for the protection of personally identifiable information (PII) or confidential information created, stored, processed, or transmitted by the Municipality of Anchorage (MOA).

2. POLICY

It is the policy of the Municipality to safeguard PII or confidential information that is maintained in any form or medium by the MOA to include computer systems, network devices and/or hard copies.

3. ORGANIZATIONS AFFECTED

All Municipal agencies.

4. REFERENCES

NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information

Alaska Statute 45.48.400 - .480 Protection of Social Security Number

Alaska Statute 45.48.010 - .090 Breach of Security Involving Personal Information

Alaska Statutes 45.48.500 - .590 Disposal of Records

Alaska Statutes 40.21.010, .070, .080.

Payment Card Industry Data Security Standard (PCI DSS)

Anchorage Municipal Code (AMC) 3.95 Records Management

5. DEFINITIONS

(1) **Confidential Information**

A property of information assets, information systems, and other resources whereby access is limited only to persons and entities authorized to view the information or access the resource.

(2) **Encryption**

A technical security control used to protect the confidentiality of an information asset.

(3) **Information Asset**

Information owned and maintained by the MOA.



Subject: <b>Protection of Personal or Confidential Information</b>	P&P No. <b>28-10</b>	<b>Page 2 of 3</b>
-----------------------------------------------------------------------	-------------------------	--------------------

(4) **Personally Identifiable Information (PII)**

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual and is protected according to law, regulation or policy.

6. RESPONSIBILITIES

- a. The Chief Information Security Officer (CISO) shall be responsible for oversight of all MOA Information security.
- b. The Departmental Directors shall:
  - (1) Ensure that PII is created, stored, processed, or transmitted for approved purposes only and in accordance with applicable legal, regulatory, and contractual requirements.
  - (2) Ensure, in conjunction with the MOA Law Department and subject to applicable laws and regulations, that individuals are informed of the unauthorized disclosure of their PII, pursuant to Alaska Statutes 45.48.010 - .090.
  - (3) Review this policy with their employees and explain where access controls or safeguards exist within their environment and who has access to those controls.
- c. The Employee shall read, acknowledge, understand, and comply with this policy.

7. PROCEDURE

- a. Social Security Numbers (SSN)
  - (1) SSN's are highly confidential and legally protected information. An SSN can only be collected if no other method of identification is available or a department has been delegated authority. Personnel must ensure SSN's are collected only when necessary and held with the strictest of confidence.
  - (2) Safeguarding of this information must comply with Alaska Statute 48.48.400 - .480 "Protection of Social Security Number".
- b. Financial Information
  - (1) Financial information is highly confidential and legally protected information. Financial account numbers, passwords, and access codes must be held with the strictest of confidence and must be secured physically or electronically to ensure the information is not disclosed to unauthorized personnel.
  - (2) Payment card data, including credit card numbers and associated information, is highly confidential and protected information. Personnel must ensure that payment card information is collected only when necessary and is handled in accordance with Payment Card Industry Data Security Standards (PCI DSS).
- c. Department of Law Notification
  - (1) In the event of unauthorized access, disclosure of PII or other confidential information, the Department of Law shall be notified.

Subject: <b>Protection of Personal or Confidential Information</b>	P&P No. <b>28-10</b>	<b>Page 3 of 3</b>
-----------------------------------------------------------------------	-------------------------	--------------------

d. Personally Identifiable Information Protection

- (1) Departmental Directors must ensure that stored PII is protected from unauthorized access or disclosure. Contact the Chief Information Security Officer (CISO) with any questions regarding the protection of your agencies personal or confidential information.
  - a. Departmental Directors must implement encryption when and wherever operationally feasible, or statutorily required, as a safeguard of electronically stored or transmitted information to include Protected Health Information, Criminal Justice Information, Credit Card and Financial Information, and Personal Information.
  - b. Departmental Directors must ensure that adequate physical controls (e.g., locked file cabinets, locked offices, controlled data center areas, computer equipment racks, audit tracking, etc.) are applied to safeguard the information.
- (2) Department Directors must ensure that all records, including PII are disposed of in accordance with MOA policies, standards, and guidelines in compliance with Alaska Statutes 45.48.500- .590 and under AMC 3.95 Records Management Ordinance.

MOA Inter

## Attachment B

**Date** : 1/18/2023 1:17:01 PM  
**From** : "Merchant, Mark A."  
**To** : "Dahl, Marc"  
**Subject** : Draft Round 2  
**Attachment** : PP\_28-41\_Internet and System Connectivity011823.docx;

FYI. Please review and add content.

*Thank you for helping us to protect our personal information.*

***Mark Merchant, CISSP, GCFA, LASO***

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)





**MUNICIPALITY OF ANCHORAGE  
OPERATING  
POLICY/PROCEDURE**

P&amp;P No.

28-41

Page 1 of 2

Effective Date:

Subject:

**Minimum security requirements for internet  
and system connectivity**

Supersedes No.

Dated:

Approved by:

1. PURPOSE

To define the minimum-security standards for internet connectivity of all Municipality of Anchorage (MOA) electronic devices and equipment. Personnel who circumvent the policy by providing unauthorized internet access to any MOA device without implementing these minimum standards are subject to disciplinary action.

The objectives of this policy are to:

- a. to provide security to the MOA networks
- b. to minimize the cost of conducting MOA business
- c. to conserve bandwidth

2. POLICY

It is the policy of the Municipality to establish and maintain a Municipal-wide standard when connecting any MOA electronic device or equipment to the internet.

3. ORGANIZATIONS AFFECTED

All Municipal agencies.

4. REFERENCES

NIST SP 800-95 Guide to Secure Web Services, NIST SP 800-53 Access Control, MOA Policy 40-16 against harassment.

5. DEFINITIONS

- a. Abused drugs - Sites that promote the abuse of both legal and illegal drugs, use and sale of drug related paraphernalia, manufacturing and/or selling of drugs.
- b. Adult - Sexually explicit material, media (including language), art, and/or products, online groups or forums that are sexually explicit in nature. Sites that promote adult services such as video/telephone conferencing, escort services, strip clubs, etc. Anything containing adult content (even if it's games or comics) will be categorized as adult.
- c. Anonymizers - Any tool that attempts to make Internet activity anonymous or untraceable, normally a proxy server interposed between a client device and the rest of the Internet.



- d. Command and Control - Command-and-control URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data
- e. Cryptocurrency - Websites that promote cryptocurrencies, crypto mining websites (but not embedded crypto miners), cryptocurrency exchanges and vendors, and websites that manage cryptocurrency wallets and ledgers. This category does not include traditional financial services websites that reference cryptocurrencies, websites that explain and describe how cryptocurrencies and blockchains work, or websites that contain embedded crypto currency miners (grayware).
- f. Dynamic DNS - Hosts and domain names for systems with dynamically assigned IP addresses and which are oftentimes used to deliver malware payloads or C2 traffic. Also, dynamic DNS domains do not go through the same vetting process as domains that are registered by a reputable domain registration company and are therefore less trustworthy.
- g. Gambling - Lottery or gambling websites that facilitate the exchange of real and/or virtual money. Related websites that provide information, tutorials or advice regarding gambling, including betting odds and pools. Corporate websites for hotels and casinos that do not enable gambling are categorized under Travel.
- h. Grayware - Web content that does not pose a direct security threat but that display other obtrusive behavior and tempt the end user to grant remote access or perform other unauthorized actions. Grayware includes illegal activities, criminal activities, rogueware, adware, and other unwanted or unsolicited applications, such as embedded crypto miners, clickjacking or hijackers that change the elements of the browser. Typosquatting domains that do not exhibit maliciousness and are not owned by the targeted domain will be categorized as grayware.
- i. Hacking - Sites relating to the illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs, how-to-advice and/or tips that may result in the compromise of networks and systems. Also includes sites that facilitate the bypass of licensing and digital rights systems.
- j. Malware - Sites known to host malware or used for command and control (C2) traffic. May also exhibit Exploit Kits.
- k. Peer to Peer - Sites that provide access to or clients for peer-to-peer sharing of torrents, download programs, media files, or other software applications. This is primarily for those sites that provide BitTorrent download capabilities.
- l. Phishing - Web content that covertly attempts to fool the user in order to harvest information, including login credentials, credit card information – voluntarily or

involuntarily, account numbers, PINs, and any information considered to be personally identifiable information (PII) from victims via social engineering techniques. Technical support scams and scareware is also included as phishing.

- m. Questionable - Websites containing tasteless humor, offensive content targeting specific demographics of individuals or groups of people.

## 6. RESPONSIBILITIES

- a. The Chief information Security Officer (CISO) shall be responsible for oversight of all MOA Information security.
- b. Records owned by the Departments are subject to oversight as designated by Executive Management under AMC 3.95.

## 7. PROCEDURE

### a. Access to Prohibited Websites

- i. Personnel must not have access to certain categories listed below will not be granted and are not accessible within the MOA networks. All categories and restricted websites may change without prior notice to adapt to evolving MOA business requirements or risk exposure to meet MOA mission and services.

#### 1. Prohibited Categories :

- Abused drugs
- Adult
- Command and Control
- Gambling
- Hacking
- Malware
- Phishing
- Questionable
- Anonymizers
- Cryptocurrency
- Dynamic -DNS
- Grayware
- Peer to Peer

### b. Access to or connection of Removeable Storage (USB) devices

- i. Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after devices have been scanned for malware.



1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)

c. Logging requirements for networked connected services

- i. Personnel connecting any servers and/or appliances into any network owned by the MOA must have authorization from ITD and must keep accurate logs of all configuration changes for XXXX years.

8. ATTACHMENTS

N/A

9. REVIEW DATE/LEAD REVIEW AGENCY

The Information Technology (IT) Department will review this document in October of each year for any needed revisions.



Municipality of Anchorage  
April 4, 2023 Regular Municipal Election  
Complaint Form

OBSERVER INFORMATION	<u>Apr. 6, 2023</u> Date
	<u>Sami Graham</u> Printed Name Of Observer
	<u>Trueblood</u> Name Of Candidate Or Organization/Group Representing

COMPLAINT	<p>SPECIFIC INFORMATION REGARDING ELECTION OFFICIAL CONDUCT OR MISCONDUCT:</p> <p>A thumb drive is used to transfer data from Dominion to an MOA computer. The process is questionable because we are not aware of a publically observable step to verify the thumb drive is actually blank. It is completely possible that the thumb drive is depositing or altering data, intentionally or unintentionally, not simply retrieving data. We request that anytime any device is connected to the Dominion machine, a qualified and mutually agreed upon member of M.O.A. IT dept. be present to supervise.</p>
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CODE CITATIONS	<p>CITATIONS TO APPLICABLE PROVISIONS OF ANCHORAGE MUNICIPAL CODE WHICH CONSTITUTES MISCONDUCT:</p> <p>Title 28. Fair &amp; honest election. The integrity of elections is important to all citizens. 'on handbook' p. 6.</p>
----------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SIGNATURES	<u>Sami Graham</u> Signature of Observer	<u>Apr. 6 '23</u> Date Submitted
	<u>Janice Klein</u> Signature of Municipal Clerk or Designee	<u>4/7/23</u> Date Received



RESPONSE TO COMPLAINT DATED APRIL 6, 2023, FILED BY SAMI GRAHAM:

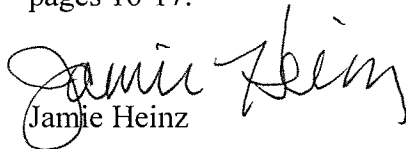
An encrypted thumb drive is inserted in the tabulations computer to download the election results which are thereafter uploaded to another computer for printing.

That thumb drive:

1. Is stored in a wall safe inside a locked room which requires a code and thumb print to open;
2. Is encrypted and reformatted each year according to Municipal IT practices; and
3. Requires a password in order to receive any download of election results.

The printed election results may be compared to the displayed computer results to ensure those results have not been changed.

The Complaint cites AMC Title 28 as authority for the alleged “misconduct.” AMC Title 28 grants authority, and responsibility, for the “overall administration of municipal elections” to the election administrator, including the “application of election related information systems, election related systems standards and procedures . . .” AMC 28.10.020C, *see* AO 2022-98, As Amended, Section 1. There is no “misconduct,” and this Complaint is treated as a suggestion related to administrative or management concerns, *see* Observer’s Handbook (12/6/2022) at pages 16-17.

  
Jamie Heinz

April 7, 2023

Gave copy to Sami Graham  
R. Duane  
4/7/23

**Date :** 4/11/2023 9:30:00 AM  
**From :** "Merchant, Mark A."  
**To :** "Dahl, Marc" [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)  
**Subject :** RE: Draft Round 2  
**Attachment :** image001.png;

This is all that's on there...

- a. Access to or connection of Removeable Storage (USB) devices
  - i. Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after devices have been scanned for malware.
    1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:59 AM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Subject:** Re: Draft Round 2

I don't see any reference to thumb drives and data exchange on critical infrastructure

Get [Outlook for iOS](#)

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:45:42 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** FW: Draft Round 2

FYI. Here was the latest draft that we did back in January.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFE*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Merchant, Mark A.  
**Sent:** Wednesday, January 18, 2023 1:17 PM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** Draft Round 2

FYI. Please review and add content.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFE, LASO*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date :** 4/11/2023 10:09:58 AM  
**From :** "Dahl, Marc" [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)  
**To :** "Merchant, Mark A." [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)  
**Subject :** RE: Draft Round 2  
**Attachment :** image001.png;

Please update to be specific on who performs the scan. For critical infrastructure the scanning needs to be limited to Security, Infrastructure or Network team or pre-registered technically capable delegate

Would also put a requirement for submittal of a formal change management(emergency if needed) and follow IT Change management process if the thumb drive content is to deliver system updates, patches, malware remediation.

**Marcus Dahl**  
**Chief Information Technology Officer**  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6<sup>th</sup> Avenue, Suite 430  
Anchorage, AK 99501  
**Office: (907) 343-6900**  
**Email: [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)**

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 9:31 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** RE: Draft Round 2

This is all that's on there...

- a. Access to or connection of Removeable Storage (USB) devices
  - i. Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after devices have been scanned for malware.
    1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:59 AM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Subject:** Re: Draft Round 2

I don't see any reference to thumb drives and data exchange on critical infrastructure

Get [Outlook for iOS](#)

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:45:42 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** FW: Draft Round 2

FYI. Here was the latest draft that we did back in January.

*Thank you for helping us to protect our personal information.*

 *Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Merchant, Mark A.  
**Sent:** Wednesday, January 18, 2023 1:17 PM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** Draft Round 2

FYI. Please review and add content.

*Thank you for helping us to protect our personal information.*

***Mark Merchant, CISSP, GCFE, LASO***  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date :** 4/11/2023 10:14:00 AM  
**From :** "Merchant, Mark A."  
**To :** "Dahl, Marc" [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)  
**Subject :** RE: Draft Round 2  
**Attachment :** image001.png;

Will do,

 I'll work on it.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFE*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 10:10 AM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Subject:** RE: Draft Round 2

Please update to be specific on who performs the scan. For critical infrastructure the scanning needs to be limited to Security, Infrastructure or Network team or pre-registered technically capable delegate

Would also put a requirement for submittal of a formal change management(emergency if needed) and follow IT Change management process if the thumb drive content is to deliver system updates, patches, malware remediation.

**Marcus Dahl**  
**Chief Information Technology Officer**  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6<sup>th</sup> Avenue, Suite 430  
Anchorage, AK 99501  
**Office: (907) 343-6900**  
**Email: [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)**

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 9:31 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** RE: Draft Round 2

This is all that's on there...

- a. Access to or connection of Removeable Storage (USB) devices
  - i. Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after devices have been scanned for malware.
    1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)

*Thank you for helping us to protect our personal information.*



*Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)



---

**From:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:59 AM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Subject:** Re: Draft Round 2

I don't see any reference to thumb drives and data exchange on critical infrastructure

Get [Outlook for iOS](#)

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:45:42 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** FW: Draft Round 2

FYI. Here was the latest draft that we did back in January.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Merchant, Mark A.  
**Sent:** Wednesday, January 18, 2023 1:17 PM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** Draft Round 2

FYI. Please review and add content.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA, LASO*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date :** 4/11/2023 10:42:48 AM  
**From :** "Dahl, Marc" [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)  
**To :** "Merchant, Mark A." [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)  
**Subject :** RE: Draft Round 2  
**Attachment :** image001.png;

Come back with what you recommend.

This is a conversation not a dictate

**Marcus Dahl**  
*Chief Information Technology Officer*  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6<sup>th</sup> Avenue, Suite 430  
Anchorage, AK 99501  
**Office:** (907) 343-6900  
**Email:** [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 10:15 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** RE: Draft Round 2

Will do,

 I'll work on it.

*Thank you for helping us to protect our personal information.*

 <p><b>INFORMATION TECHNOLOGY DEPARTMENT</b></p>	<p><i>Mark Merchant, CISSP, GCFA</i> Chief Information Security Officer MOA/Security Services P: 907-343-6917 C: 907-305-3033 E: <a href="mailto:mark.merchant@anchorageak.gov">mark.merchant@anchorageak.gov</a></p>
---------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

**From:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 10:10 AM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Subject:** RE: Draft Round 2

Please update to be specific on who performs the scan. For critical infrastructure the scanning needs to be limited to Security, Infrastructure or Network team or pre-registered technically capable delegate

Would also put a requirement for submittal of a formal change management(emergency if needed) and follow IT Change management process if the thumb drive content is to deliver system updates, patches, malware remediation.

**Marcus Dahl**  
**Chief Information Technology Officer**  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6<sup>th</sup> Avenue, Suite 430  
Anchorage, AK 99501  
**Office: (907) 343-6900**  
**Email: [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)**

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 9:31 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** RE: Draft Round 2

This is all that's on there...

- a. Access to or connection of Removeable Storage (USB) devices
  - i. Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after devices have been scanned for malware.
    1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:59 AM  
**To:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Subject:** Re: Draft Round 2

I don't see any reference to thumb drives and data exchange on critical infrastructure

Get [Outlook for iOS](#)

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 8:45:42 AM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** FW: Draft Round 2

FYI. Here was the latest draft that we did back in January.

*Thank you for helping us to protect our personal information.*

 *Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Merchant, Mark A.  
**Sent:** Wednesday, January 18, 2023 1:17 PM  
**To:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** Draft Round 2

FYI. Please review and add content.

*Thank you for helping us to protect our personal information.*

***Mark Merchant, CISSP, GCFA, LASO***

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date : 4/11/2023 12:16:00 PM**  
**From : "Merchant, Mark A."**  
**To : "Dahl, Marc" [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)**  
**Subject : Latest Draft for website.**  
**Attachment : image001.png;**

Getting close...

Access to or connection of Removeable Storage (USB) devices

Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.

1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)
2. Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.

(Link to Change Management Procedures)

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date :** 4/11/2023 1:20:00 PM  
**From :** "Merchant, Mark A."  
**To :** "Holland, Heather M." heather.holland@anchorageak.gov  
**Cc :** "Dahl, Marc" marcus.dahl@anchorageak.gov  
**Subject :** ITD Policy Statements  
**Attachment :** image001.png;

Good afternoon, Heather.

Can you please add a new link on this page...

<https://anchorageak.sharepoint.com/sites/CyberSecurity> called "ITD Policy Statements."

Then on the ITD Policy Statements page I would like to add this language to start off and then we can add other IT policy statements as well. All statements must be approved by the Director prior to posting. This is one Marc would like to put up as soon as possible.

#### Access to or connection of Removeable Storage (USB) devices

Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.

1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)
2. Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)





**Date :** 4/11/2023 1:31:19 PM  
**From :** "Holland, Heather M." heather.holland@anchorageak.gov  
**To :** "Merchant, Mark A." mark.merchant@anchorageak.gov  
**Cc :** "Dahl, Marc" marcus.dahl@anchorageak.gov  
**Subject :** RE: ITD Policy Statements  
**Attachment :** image002.png;image003.png;

Good afternoon Mark,  
Sure thing, the new page is at  
<https://anchorageak.sharepoint.com/sites/CyberSecurity/SitePages/ITD-Policy-Statements.aspx>  
I have added a link in the Additional Information and External Sites listing, please let me know what you would like to have adjusted.

Thank you!

**Heather Holland**  
*System Analyst*  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6th Avenue, Suite 430  
Anchorage, AK 99501  
**Phone** 907.343.6899  
**Email** [heather.holland@anchorageak.gov](mailto:heather.holland@anchorageak.gov)

---

**From:** Merchant, Mark A. <mark.merchant@anchorageak.gov>  
**Sent:** Tuesday, April 11, 2023 1:20 PM  
**To:** Holland, Heather M. <heather.holland@anchorageak.gov>  
**Cc:** Dahl, Marc <marcus.dahl@anchorageak.gov>  
**Subject:** ITD Policy Statements

Good afternoon, Heather.

Can you please add a new link on this page...  
<https://anchorageak.sharepoint.com/sites/CyberSecurity> called "ITD Policy Statements."

Then on the ITD Policy Statements page I would like to add this language to start off and then we can add other IT policy statements as well. All statements must be approved by the Director prior to posting. This is one Marc would like to put up as soon as possible.

Access to or connection of Removeable Storage (USB) devices

Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical

infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.

1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)
2. Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date :** 4/11/2023 1:34:00 PM  
**From :** "Merchant, Mark A."  
**To :** "Holland, Heather M." heather.holland@anchorageak.gov  
**Cc :** "Dahl, Marc" marcus.dahl@anchorageak.gov  
**Subject :** RE: ITD Policy Statements  
**Attachment :** image001.png;image002.png;

Wow! That was fast. I'll talk to Marc about your bonus. 😊

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*

Chief Information Security Officer

MOA/Security Services

P: 907-343-6917

C: 907-305-3033

E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

---

**From:** Holland, Heather M. <heather.holland@anchorageak.gov>  
**Sent:** Tuesday, April 11, 2023 1:31 PM  
**To:** Merchant, Mark A. <mark.merchant@anchorageak.gov>  
**Cc:** Dahl, Marc <marcus.dahl@anchorageak.gov>  
**Subject:** RE: ITD Policy Statements

Good afternoon Mark,

Sure thing, the new page is at

<https://anchorageak.sharepoint.com/sites/CyberSecurity/SitePages/ITD-Policy-Statements.aspx>

I have added a link in the Additional Information and External Sites listing, please let me know what you would like to have adjusted.

Thank you!

**Heather Holland**

*System Analyst*

**Municipality of Anchorage**

**Information Technology Department**

632 W 6th Avenue, Suite 430

Anchorage, AK 99501

**Phone** 907.343.6899

**Email** [heather.holland@anchorageak.gov](mailto:heather.holland@anchorageak.gov)

---

**From:** Merchant, Mark A. <[mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)>  
**Sent:** Tuesday, April 11, 2023 1:20 PM  
**To:** Holland, Heather M. <[heather.holland@anchorageak.gov](mailto:heather.holland@anchorageak.gov)>  
**Cc:** Dahl, Marc <[marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)>  
**Subject:** ITD Policy Statements

Good afternoon, Heather.

Can you please add a new link on this page....

<https://anchorageak.sharepoint.com/sites/CyberSecurity> called "ITD Policy Statements."

Then on the ITD Policy Statements page I would like to add this language to start off and then we can add other IT policy statements as well. All statements must be approved by the Director prior to posting. This is one Marc would like to put up as soon as possible.

#### Access to or connection of Removeable Storage (USB) devices

Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.

1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)
2. Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.

*Thank you for helping us to protect our personal information.*

*Mark Merchant, CISSP, GCFA*  
Chief Information Security Officer  
MOA/Security Services  
P: 907-343-6917  
C: 907-305-3033  
E: [mark.merchant@anchorageak.gov](mailto:mark.merchant@anchorageak.gov)

**Date :** 4/11/2023 2:00:00 PM  
**From :** "Dahl, Marc"  
**To :** "Dahl, Marc" [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)  
**Subject :** IT USB Policy  
**Attachment :** image001.png;

[ITD Policy Statements \(sharepoint.com\)](#)

## **ITD Policy Statements**

### **Access to or connection of Removeable Storage (USB) devices**

Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.

1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)
2. Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.

**Marcus Dahl**  
**Chief Information Technology Officer**  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6<sup>th</sup> Avenue, Suite 430  
Anchorage, AK 99501  
**Office: (907) 343-6900**  
**Email: [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)**



**Date :** 4/11/2023 2:37:00 PM  
**From :** "Dahl, Marc"  
**To :** "alaskansam@yahoo.com" alaskansam@yahoo.com  
**Subject :** IT USB Policy  
**Attachment :** image001.png;

Published on the internal IT Security web page [ITD Policy Statements \(sharepoint.com\)](#)

## **ITD Policy Statements**

### **Access to or connection of Removeable Storage (USB) devices**

Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.

1. USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)
2. Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.

**Marcus Dahl**  
**Chief Information Technology Officer**  
**Municipality of Anchorage**  
**Information Technology Department**  
632 W 6<sup>th</sup> Avenue, Suite 430  
Anchorage, AK 99501  
**Office:** (907) 343-6900  
**Email:** [marcus.dahl@anchorageak.gov](mailto:marcus.dahl@anchorageak.gov)



Municipality of Anchorage  
April 4, 2023 Regular Municipal Election

Election Commission - Failure to Comply with Law or Alleged Illegal Election Practices

OBSERVER INFORMATION	April 11, 2023 Date
	Sami Graham / DANIEL E. SMITH / JOHN HENRY Printed Name Of Observer
	Trueblood Name Of Candidate Or Organization/Group Representing

EXPLANATION OF EVENTS	EXPLANATION OF ALL EVENTS CREATING THE CONCERN: As an appeal to comments received on Apr. 6, 2023, from Jamie Heinz, and references to MOA ITD practices, according to MOA ITD policy statement Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from The Information Technology Dept (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD change management processes and procedures regarding patch management & malware remediation.
	We believe the clerk's current practices in relation to

CODE CITATIONS	CITATIONS TO APPLICABLE PROVISIONS OF ANCHORAGE MUNICIPAL CODE WHICH WERE NOT COMPLIED WITH: MOA ITD USB Policy Statement - regarding election clerk's response #2, dated April 7, '23

AFFECTS TO OUTCOME OF ELECTION	<p>EXPLANATION OF HOW THE CONCERN WOULD CHANGE THE OUTCOME OF THE ELECTION IF FOUND TO BE TRUE:</p> <p>It is completely possible that the USB device is depositing or altering data, intentionally or unintentionally, not simply retrieving data, thereby nullifying the results of the election.</p> <p>"Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to municipal operations and or resources."</p>
--------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SIGNATURES	<p><i>Sabri N. Khan</i> <i>Paul E. Smith</i> <i>John L. King</i></p> <p>Signature of Observer <span style="float: right;">Date Submitted</span></p> <p style="text-align: right;">Apr. 11, 2023</p>
	<p>Signature of Municipal Clerk or Designee <span style="float: right;">Date Received</span></p>

**Date : 4/14/2023 11:31:00 AM**  
**From : "Dahl, Marc"**  
**To : "alaskansam@yahoo.com" alaskansam@yahoo.com**  
**Subject : FW: 04182023S Municipal Assembly Agenda - FINAL**

See this proposed code update being introduced at the next assembly.

5.A. Ordinance No. AO 2023-45, an ordinance of the Anchorage Assembly amending Anchorage Municipal Code Section (AMC) 2.30.020 to recognize the decision making authority of the assembly with respect to uncodified mayoral directives, policies and procedures, and other uncodified policies and administrative practices as applied to the legislative branch, and amending AMC section 3.50.010 accordingly, Assembly Vice-Chair Constant.

-----Original Message-----

From: Sleppy, Karissa M. <karissa.sleppy@anchorageak.gov>  
Sent: Friday, April 14, 2023 10:41 AM  
Subject: 04182023S Municipal Assembly Agenda - FINAL  
Importance: High

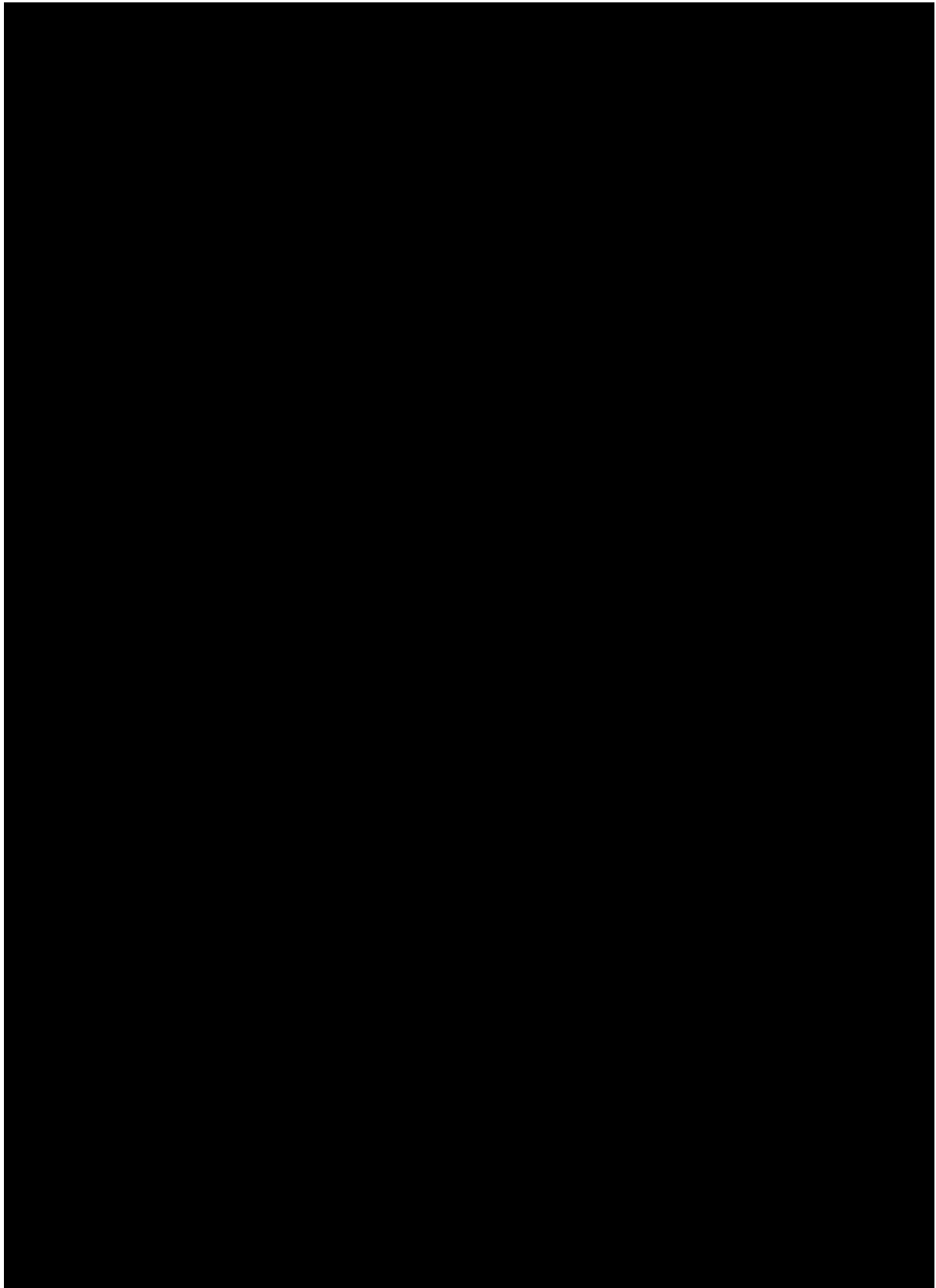
Your message is ready to be sent with the following file or link attachments:

04182023S\_Final

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

**Date : 4/14/2023 1:29:00 PM**  
**From : "Dahl, Marc"**  
**To : "Helzer, Anne" Anne.Helzer@anchorageak.gov**  
**Subject : FW: 04182023S Municipal Assembly Agenda - FINAL**

Anne,







Municipality of Anchorage  
April 4, 2023 Regular Municipal Election

Election Commission – Failure to Comply with Law or Alleged Illegal Election Practices

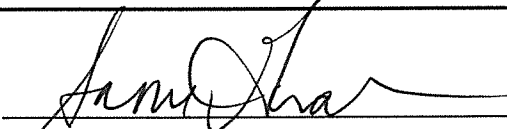
OBSERVER INFORMATION	Apr. 14, 2023 Date
	Sami Graham Printed Name Of Observer
	Trueblood Name Of Candidate Or Organization/Group Representing

EXPLANATION OF EVENTS	<p>EXPLANATION OF ALL EVENTS CREATING THE CONCERN:</p> <p>An appeal dated April 11, 2023, appealing a challenge dated Apr. 6, 23 concerning the practice of inserting a thumb drive into the Dominion System to transfer election data to a municipal computer. The appeal was raised because the clerks office stated they were following MOA ITD. policy and yet they are in direct violation of MOA ITD USB policy. On Friday, April 14, 23 The Assembly item 15.A. No. 2023-45, written by Christopher Constant - a candidate in the current election - is a direct response to the appeal dated Apr. 11. It changes the processes and procedures of an election during the middle of an election.</p>
-----------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CODE CITATIONS	<p>CITATIONS TO APPLICABLE PROVISIONS OF ANCHORAGE MUNICIPAL CODE WHICH WERE NOT COMPLIED WITH:</p> <p>How did Christopher Constant get information concerning an appeal that was supposed to go to the Election Commission?</p>
	<p>MOA ITD. USB Policy Statement</p>



AFFECTS TO OUTCOME OF ELECTION	EXPLANATION OF HOW THE CONCERN WOULD CHANGE THE OUTCOME OF THE ELECTION IF FOUND TO BE TRUE: Again: It is completely possible that the USB device is depositing or altering data, intentionally or unintentionally, not simply retrieving data, thereby nullifying the results of the election. "Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to municipal operations and on resources." Why would the clerk refuse to allow the IT Dept. to follow policy/procedures?
--------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SIGNATURES	 Signature of Observer	APR. 14, 23 Date Submitted
	Signature of Municipal Clerk or Designee	Date Received

**From:** Heinz, Jamie L.  
**Sent:** Sunday, April 16, 2023 12:07 PM  
**To:** alaskansam@yahoo.com  
**Cc:** emerald1@alaska.net; Brenda Hastie; J H; Jones, Barbara A.  
**Subject:** 2nd Appeal Re. Thumb Drive  
**Attachments:** 2nd appeal.pdf; FW: Notification: Agenda Deadline Reminder for April 7, 2023 Special;  
FW: 04072023S Municipal Assembly Agenda - FINAL

Dear Ms. Graham,

This email is in response to your second appeal regarding the thumb drive, which was filed on Friday, April 14<sup>th</sup>. In this second appeal, you note AO 2023-45 as item 5.A. on the Special Meeting Agenda for Tuesday, April 18<sup>th</sup>. Please note that the items up for public hearing at the April 18<sup>th</sup> meeting were introduced at the April 7<sup>th</sup> Special Meeting. Attached, you will find an email stating that the agenda deadline for items to be submitted to the Clerk's Office for inclusion in the April 7<sup>th</sup> Special Meeting was noon on Wednesday, April 5<sup>th</sup>. Also attached, you will find an email, sent out at 10:57 a.m. on Thursday, April 6<sup>th</sup>, which provides the entire packet of materials for the April 7<sup>th</sup> Special Meeting. You will see included in that packet, item 6.A., AO 2023-45.

This ordinance was in the works and submitted to the Clerk's Office before noon on Wednesday, April 5<sup>th</sup> which is before your initial complaint was submitted the afternoon of April 6<sup>th</sup> and the timing is purely coincidence.

Jamie



**Jamie Heinz, MMC**  
Election Administrator  
**Municipality of Anchorage Elections**  
907-343-4320  
[www.muni.org/elections](http://www.muni.org/elections)

**MOA Elections Mission:** *We believe in fair, accurate, and accessible elections. In order to increase voter turnout, we serve and educate the community, election workers, and others, we work to increase public participation in the democratic process of local government. Ver. 1.0*

*Messages to and from this email address may be available to the public under Alaska Public Records Law.*

**From:** [Veneklasen, Jennifer O.](#)  
**To:** [Heinz, Jamie L.](#)  
**Subject:** FW: 04072023S Municipal Assembly Agenda - FINAL  
**Date:** Friday, April 14, 2023 3:40:43 PM  
**Attachments:** [Assembly - Special - Meeting Packet - 4-7-2023 \(4-6-2023 9 19 51 AM\).pdf](#)  
**Importance:** High

---

This is when the assembly meeting packet materials were sent to members and administration, as well as published online.

-----Original Message-----

**From:** Sleppy, Karissa M. <karissa.sleppy@anchorageak.gov>  
**Sent:** Thursday, April 6, 2023 10:57 AM  
**Subject:** 04072023S Municipal Assembly Agenda - FINAL  
**Importance:** High

Your message is ready to be sent with the following file or link attachments:

04072023S\_Final  
Agenda and packet included

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

**From:** [Veneklasen, Jennifer O.](#)  
**To:** [Heinz, Jamie L.](#)  
**Subject:** FW: Notification: Agenda Deadline Reminder for April 7, 2023 Special  
**Date:** Friday, April 14, 2023 3:39:26 PM  
**Importance:** High

---

**From:** Sleppy, Karissa M. <karissa.sleppy@anchorageak.gov>  
**Sent:** Tuesday, April 4, 2023 10:19 AM  
**To:** !MAS Municipal Clerk <MASMunicipalClerk@anchorageak.gov>; !MAS Assembly Counsel <MASAssemblyCounsel@anchorageak.gov>; !MAS Assembly Members <!MASAssemblyMembers@anchorageak.gov>; !MAS Ombudsman <MASOmbudsman@anchorageak.gov>; Assembly Legislative Services <wwmasls@anchorageak.gov>  
**Cc:** Kohlhase, Kent E. <kent.kohlhase@anchorageak.gov>; Hickel, Kolby A. <Kolby.Hickel@anchorageak.gov>; Trombley, Adam R. <Adam.Trombley@anchorageak.gov>  
**Subject:** Notification: Agenda Deadline Reminder for April 7, 2023 Special  
**Importance:** High

**REMINDER:** The deadline for item placement on the April 7, 2023 Special agenda is **NO LATER THAN NOON on Wednesday, April 5, 2023**. This meeting is for introduction of ordinances and any time-sensitive purchasing-related items, with the potential to schedule a Special Meeting on April 18 to take up the public hearing items.

Also, **please submit your items in OnBase**. The April 7<sup>th</sup> meeting has been created and is open for submissions.

Your cooperation is appreciated.



Sincerely,  
**Karissa Sleppy**  
Agenda Assistant

***Municipality of Anchorage***  
Municipal Clerk's Office  
907-343-4311

*Messages to and from this email address may be available to the public under Alaska Public Records Law.*

**From:** Sami Graham <alaskansam@yahoo.com>  
**Sent:** Sunday, April 16, 2023 4:16 PM  
**To:** Heinz, Jamie L.  
**Subject:** Re: 2nd Appeal Re. Thumb Drive

**[EXTERNAL EMAIL]**

Jamie,

Thank you. I withdraw my challenge dated April 14.

Sami Graham

Sent from my iPhone

On Apr 16, 2023, at 12:07 PM, Heinz, Jamie L. <jamie.heinz@anchorageak.gov> wrote:

Dear Ms. Graham,

This email is in response to your second appeal regarding the thumb drive, which was filed on Friday, April 14<sup>th</sup>. In this second appeal, you note AO 2023-45 as item 5.A. on the Special Meeting Agenda for Tuesday, April 18<sup>th</sup>. Please note that the items up for public hearing at the April 18<sup>th</sup> meeting were introduced at the April 7<sup>th</sup> Special Meeting. Attached, you will find an email stating that the agenda deadline for items to be submitted to the Clerk's Office for inclusion in the April 7<sup>th</sup> Special Meeting was noon on Wednesday, April 5<sup>th</sup>. Also attached, you will find an email, sent out at 10:57 a.m. on Thursday, April 6<sup>th</sup>, which provides the entire packet of materials for the April 7<sup>th</sup> Special Meeting. You will see included in that packet, item 6.A., AO 2023-45.

This ordinance was in the works and submitted to the Clerk's Office before noon on Wednesday, April 5<sup>th</sup> which is before your initial complaint was submitted the afternoon of April 6<sup>th</sup> and the timing is purely coincidence.

Jamie

[<image003.png>](#)

**Jamie Heinz, MMC**  
Election Administrator

**Municipality of Anchorage Elections**  
907-343-4320  
[www.muni.org/elections](http://www.muni.org/elections)

## Attachment K

**MOA Elections Mission:** *We believe in fair, accurate, and accessible elections. In order to increase voter turnout, we serve and educate election workers, and others, we work to increase public participation in the democratic process of local government. Ver. 1.0*

*Messages to and from this email address may be available to the public under Alaska Public Records Law.*

<2nd appeal.pdf>

<mime-attachment>

<mime-attachment>



# Anchorage Election Commission Public Session of Canvass and Adoption of the Election Canvass Report

April 20, 2023

5:00 p.m. until complete

## AGENDA - Revised

In person:  
MOA Election Center  
619 East Ship Creek Avenue, Door D  
Anchorage, AK 99501

For the public to dial in:  
Conference Bridge Phone Number –  
(907) 273-5190  
Participant Code – 786815 #

### 1. Call to Order

### 2. Roll Call

**Lisa Torkelson – Chair**  
Loren Leman – Vice Chair  
Glennis Ireland  
Mead Treadwell

### 3. Minutes of Previous Meetings

- A. Minutes of the Anchorage Election Commission Meeting of January 11, 2023

### 4. Old Business

### 5. New Business

- A. Disclosures
- B. Review of Pending Rejected Ballot Envelopes
- C. Complaints
  - a. *The Election Commission – Failure to Comply with Law or Alleged Illegal Election Practices re MOA ITD USB Policy Statement*
  - b. *The Election Commission – Failure to Comply with Law or Alleged Illegal Election Practices re Mailing Ballots to Registered Voters*
- D. Adoption of the Election Canvass Report for the Regular Municipal Election of April 4, 2023 \*

\* **STAFF NOTE:** After the motion to adopt the Election Canvass Report, the Commission will **take a short recess** before signing the Election Canvass Report.

### 6. Member Comments

### 7. Audience Participation

### 8. Adjournment



# Municipality of Anchorage

P.O. Box 196650 • Anchorage, Alaska 99519-6650 • Telephone: (907) 343-4311 • Fax: (907) 343-4313 • <http://www.muni.org/assembly>

## Anchorage Assembly Leadership

July 5, 2023

Mayor Dave Bronson  
632 W. 6<sup>th</sup> Ave., Suite 850  
Anchorage, AK 99501

Re: Advance Notice of Questions to be Addressed at July 21 Worksession—  
*April 11 Election Complaint and Creation of ITD Policy Statement Regarding  
Removable Storage Devices*

Mayor Bronson:

The Assembly has scheduled a worksession for Friday, July 21 to discuss the election complaint received by the Municipality on April 11, 2023.<sup>1</sup> The complaint quoted, verbatim, from a purported municipal “ITD Policy Statement” that was created and published only on a non-public municipal website mere hours before the complaint was submitted.<sup>2</sup> Exactly how the authors of the election complaint came to have a copy of the “policy” has generated significant public interest.<sup>3</sup>

We invite representatives of your administration to attend the worksession.

---

<sup>1</sup> See Sami Graham, Daniel E. Smith, John Henry, Renewed Election Complaint (April 11, 2023), attached as Exhibit A. Compare MUNICIPALITY OF ANCHORAGE, MUNICIPAL CLERK’S OFFICE, [Election] *Observer’s Handbook* at 17 (Oct. 13, 2022) (“Complaints that are not resolved by the Municipal Clerk or Election Administrator and that would change the outcome of the election, if found to be true, may be renewed by the observer or candidate. The renewed complaint shall be submitted to the Election Administrator in writing on a form entitled – ‘Election Commission – Alleged Failure to Comply with Law or Alleged Illegal Election Practices’.”); see also AR 222-328 *A Resolution of The Anchorage Municipal Assembly Updating and Amending the Election Observer’s Handbook and Associated Forms*.

<sup>2</sup> See, ITD Policy Statement and List Showing Uploaded Time and Date (April 11, 2023), attached as Exhibit B. See also Emily Goodykoontz, *Former Top Aide To Mayor Challenged Anchorage Election Using Policy Quietly Added That Day By City IT Director*, ANCHORAGE DAILY NEWS (May, 20, 2023), available at: <https://www.adn.com/alaska-news/anchorage/2023/05/20/former-top-aide-to-mayor-challenged-anchorage-election-using-policy-quietly-added-that-day-by-city-it-director/>

<sup>3</sup> See, e.g., Editorial, *Anchorage Residents Deserve To Know: What Was That Shady Municipal Election Complaint About?* ANCHORAGE DAILY NEWS (June 17, 2023), available at: <https://www.adn.com/opinions/editorials/2023/06/17/editorial-anchorage-residents-deserve-to-know-what-was-that-shady-municipal-election-complaint-about/>



To ensure that the worksession is maximally productive, we wish to provide you and your administration with advance notice of the topics we wish to cover.

1. **Origin of the Purported Policy.** The purported “ITD Policy Statement” referenced by the renewed election complaint was not an official municipal operating policy or procedure. Official municipal policies and procedures must, among other things, be reviewed and approved by the Office of Management and Budget, the Municipal Attorney, the Municipal Manager, and signed by the Mayor.<sup>4</sup> The policy was also unworkable in practice and, if applied to processes at the Election Center, would have needlessly added risk to the security protocols that ensure the integrity of local elections.<sup>5</sup>

The first topic that the Assembly wishes to explore is how the “ITD Policy Statement” was developed:

- Was the Statement drafted through any kind of a deliberative process? If so, what did that process entail?
- Who was involved in the development of the Statement?
- What persons were involved in posting the statement to the Municipality’s internal website?

---

<sup>4</sup> See Municipality of Anchorage, P&P No. 1 *Municipal Operating Policies and Procedures* (Dec. 17, 1996) at § 7(c)(6) (“OMB will forward the final document to the Municipal Attorney for legal review, the Municipal Manager for review and then to the Mayor for signature”).

<sup>5</sup> A thumb drive is currently used to transport vote counts from the municipality’s scanning, adjudication, and tabulation system, which is “air gapped,” to municipal computers that are used to report election results. When it was first procured, the thumb drive was obtained from and formatted by the municipal IT department and encrypted.

To ensure that the thumb drive could not be subsequently tampered with, the drive is stored in a locked safe, in a locked room that requires a code and thumb print to open, and the password for the thumb drive is known to an extremely limited number of individuals.

To ensure that the thumb drive is merely moving vote counts from one machine to another, and not otherwise having an effect on the election process, vote totals are displayed on the ballot-scanning machine both before and after the thumb drive is inserted (and can be observed not to have changed after the thumb drive is inserted); and published election results are seen to correspond to the totals displayed on the ballot-scanning machine.

Last, to ensure that the ballot-scanning machine is itself correctly displaying accurate vote counts, the Municipality conducts a “risk limiting audit.” As further detailed in the memorandum attached to AM 324-2023 (*see* page 395-404), the audit entails hand counting randomly selected ballots in batches (using dice to seed a random-number generator), and comparing the results of the hand count to totals reported by the machine. In the 2023 municipal election, 3,200 ballots were randomly selected for hand counting, and “the hand count and machine count of those ballots was identical.” AM 324-2023 at 402.

**2. Extent of Administration Involvement in the Complaint.** The renewed election complaint was submitted by your former chief of staff, Sami Graham, and two other individuals,<sup>6</sup> and the content of the complaint has led members of the public to conclude that the complaints must have been in communication with the municipal information technology department. As the Anchorage Daily News editorial board put it:

There are surely a number of explanations for how Bronson administration ally and former chief of staff Sami Graham came to file an election complaint that cited a computer policy only hours old that didn't exist in any public form, but the simplest one is that the complaint was the result of coordination between Graham and administration officials. And the circumstances of that seeming coordination are cause for grave concern.

. . . the real red flag about the IT policy is that there's no reason Graham and her compatriots should have known it even existed. It had been added to the municipality's internal network by municipal IT director Marc Dahl on April 11, only two hours before Graham's complaint was filed, and the policy was not accessible by the public. None of the people making the complaint had any means of accessing the policy, but they somehow quoted it verbatim.

Also notable: The policy didn't exist at the time Graham said municipal elections employees had violated it (April 6 and 7), and Heinz said no elections personnel had been made aware of its existence before the complaint.<sup>7</sup>

The second topic the Assembly wishes to explore is whether and how municipal employees communicated (and/or coordinated) with the complainants about the "ITD Policy Statement" and/or the election complaint:

- What non-municipal employees were informed about the existence (or substance) of the "ITD Policy Statement," prior to April 12?
- What contact did the complainants have with municipal staff, such that they were aware of the "ITD Policy Statement" and its exact language? Who was involved in the communications, and when and how did they occur?

To the extent that any such communications were conducted by email or otherwise memorialized, the Assembly requests copies of the emails and memorializations, all of which are likely to be non-confidential public records.

---

<sup>6</sup> See Exhibit A.

<sup>7</sup> See Editorial, above at n.3.


3. Management Awareness. The final topic that the Assembly wishes to explore is the extent to which municipal management was aware that the ITD Policy Statement was being developed, or discussed with complainants.

- Were you, or any member of the Mayor's office, aware of the ITD Policy Statement before the Statement was posted on April 11?
- To what extent, if any, were you, or any member of the Mayor's office, involved in the development of the ITD Policy Statement?
- Were you, or any member of the Mayor's office, aware of the April 11 election complaint that referenced the ITD Policy Statement before the complaint was submitted?
- To what extent, if any, were you, or any member of the Mayor's office, involved in the development of the April 11 election complaint that referenced the ITD Policy Statement?

\* \* \* \* \*

Thank you for your attention to this matter. We hope the Administration will participate in the worksession on Friday, July 21, from 10:00am to 11:30am. If you have any questions, we would be happy to discuss.

Sincerely,



Christopher Constant, Chair



Meg Zaletel, Assembly Vice Chair

Cc: Anne Helzer-Municipal Attorney  
Kent Kohlhasse - Municipal Manager  
Mario Bird - Chief of Staff  
Philippe Brice - Acting ITD Director  
Anchorage Assembly

## Attachment N

**From:** [Constant, Christopher](#)  
**To:** [Helzer, Anne](#)  
**Cc:** [Gates, Dean T.](#); [Hurt, Matthew P.](#); [Heasley, Brandi M.](#); [Willoughby, Jessica B.](#)  
**Subject:** Records Request  
**Date:** Monday, July 10, 2023 12:38:22 PM

---

Hi Anne,

I am not sure the exact protocol for making this request. I am seeking copies of the records provided to the Ombudsman relating to communications between Sami Graham, Mark Merchant, Heather Holland, and Marc Dahl. I understand I need to make this request to the department head. I am hoping you will facilitate this for me. We have a worksession on Friday July 21 and the communications are timely. The specific search terms are below.

Very respectfully,

Christopher Constant

The specific terms were as follows and are incorporated as the terms of this request:

MOA Email Inboxes – To, From, or Between these email addresses that contain any of the keywords listed below

- [Marcus.Dahl@anchorageak.gov](mailto:Marcus.Dahl@anchorageak.gov)
- [Mark.Merchant@anchorageak.gov](mailto:Mark.Merchant@anchorageak.gov)
- [Heather.Holland@anchorageak.gov](mailto:Heather.Holland@anchorageak.gov)

External Email Inboxes – To, From, or Between the MOA email addresses listed above and the external email addresses listed below

- [Alaskangraham@yahoo.com](mailto:Alaskangraham@yahoo.com)
- [Alaskansam@yahoo.com](mailto:Alaskansam@yahoo.com)

Date Range

- March 15,2023 – April 23, 2023

Keywords

• USB, Policy, Election, Trueblood, Appeal, Challenge, Clerk, Commission, Thumb Drive, Dominion, Computer

Additional Information Requested

• Any text messages between Marc Dahl's MOA cell phone and 907-230-9034 between March 15, 2023 and April 23, 2023

August 17, 2023

## **Final Investigative Report Concerning Ombudsman Complaint 2023-0550**

### **COMPLAINT**

On April 26, 2023, following the April 20<sup>th</sup> Anchorage Election Commission’s Public Session of Canvass and Adoption of the Election Canvass Report, a constituent contacted the Ombudsman. The constituent questioned, based on comments by the Election Administrator and other members of the election team during the Commission meeting, whether the Director of the Municipality’s Office of Information Technology had developed and posted an OIT USB policy in order to provide support for an election observer’s challenge of the April 4, 2023 Municipal election, with the intent of overturning the election results.

### **FINDINGS**

The complaint involving the Director of the Municipality of Anchorage’s Office of Information Technology is **JUSTIFIED**.

### **BACKGROUND AND TIMELINE**

April 26, 2023, a constituent contacted the Ombudsman to express their concerns regarding the alleged actions of the Director of the Municipality’s Office of Information Technology (OIT). The constituent had listened to the April 20<sup>th</sup> Anchorage Election Commission’s (Commission) Public Session of Canvass and Adoption of the Election Canvass Report. During the meeting an election observer discussed an election challenge they had filed with the Commission regarding the use of USB drives by the election team. Based on comments made by the Election Administrator and other members of the election team, the constituent questioned if the Director had developed and posted an OIT USB policy to provide support for the election challenge. The policy had been posted on the OIT intranet the same day that the challenge was filed.

During his investigation, the Ombudsman reviewed relevant emails, memoranda, policies, codes, photos, and videos. The Ombudsman reviewed 1,500+ documents that were provided in response to his records request, which did not contain the redactions that were in the documents provided to the Assembly Chair and the media. The Ombudsman also spoke with multiple members of OIT staff, and former members of OIT staff.

The Ombudsman determined that for several years, across multiple administrations and Directors, OIT had an internal policy that required that OIT staff could not insert USB drives into



MOA equipment unless the drives were scanned by OIT personnel. This policy was internal to OIT and did not have MOA-wide applications. MOA Policy & Procedure 1-1, signed by Mayor Mystrom on April 8, 1997, requires that the development of any policy with MOA - wide applications be developed through a collaborative process involving all department directors and department policy coordinators, and the Office of Management & Budget (OMB), which is tasked with assigning a P&P number to the final, posted document, that has been signed by the Mayor. P&P 1-1 also requires that any new policy must include procedures for implementing the policy, and that MOA employees be informed regarding the policy.

During his review, the Ombudsman determined that the requirements of P&P 1-1 were not followed in developing the OIT USB policy that was posted on the OIT intranet at 1:28 pm on April 11, 2023. The OMB Director informed the Ombudsman that she was unaware of the policy's existence until she was contacted by the Ombudsman. The OIT Chief Information Security Officer (CISO) acknowledged to the Ombudsman that the policy posted on the OIT Policy Statements page was an internal OIT policy and was not an MOA-wide policy.

To assist in understanding the chain of events related to this matter, the Ombudsman developed a timeline –

- Fall 2022: OIT staff hold discussions regarding turning a long-standing OIT internal policy that requires that any USB drive inserted into any MOA asset be scanned by OIT staff into an MOA-wide policy. A draft policy is developed (28-41) that includes language that states “Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after devices have been scanned for malware.” The conversation goes dormant in January 2023.
- 03/22/2023: The MOA Records Specialist emailed a link to Policy & Procedure 1-1 to the OIT Director, Marc Dahl. P&P 1-1 outlines the process for developing policies and procedures with MOA-wide applications. Policy & Procedure 1-1 was signed by Mayor Mystrom on April 8, 1997.
- 04/06/2023: Sami Graham, an election observer with the Trueblood campaign, filed a complaint regarding the 04/04/2023 Municipal election. Graham expresses concerns that a thumb drive is used to transfer data from Dominion equipment to an MOA computer. She stated that there is no way to know if the thumb drive is blank. The complaint form stated that “We request that anytime any device is connected to the Dominion machine a qualified and mutually agreed upon member of M.O.A. IT dept. be present to supervise”.
- 04/07/2023: MOA Election Administrator Jamie Heinz responds to Graham’s complaint, and notes that the Election’s thumb drives 1. Are stored in a wall safe inside a locked room which requires a code and thumb print to open; 2. Are encrypted and reformatted each year according to Municipal IT practices; and 3. Require a password to receive any download of election results. Heinz determined that there was no “misconduct”, and that the complaint would be treated as a suggestion related to administrative or management concerns.

- 04/11/2023: The morning of April 11, 2023, Dahl contacts the CISO to restart the conversation regarding developing a USB policy. At 8:42 am, the CISO emails the January 2023 policy draft to Dahl. Dahl and the CISO exchange several emails regarding the language for the policy. Dahl noted that he did not see any reference to thumb drives and data exchange on critical infrastructure – language is added to the draft policy. After the language is added Dahl directs that the revised policy be posted on the OIT intranet page.
- 04/11/2023: A new OIT “Policy Statements” page is created, and the USB policy is posted on the MOA intranet at 1:28 pm. An OIT employee was instructed to create the page and post the policy by the CISO, at the behest of Director Dahl –  
**Access to or Connection of Removeable Storage (USB) devices**  
*Personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the Information Technology Department (ITD) and only after the USB devices have been scanned for malware by ITD. All insertions into MOA critical infrastructure technology must also be approved and/or observed by ITD management and must follow ITD Change management processes and procedures regarding patch management and malware remediation.*
  1. *USB devices includes any external device that utilizes a USB connection type (i.e., Type-A, Type-B, Mini USB, Micro USB, Type-C, USB 2.0, 3.0, etc.)*
  2. *Critical Infrastructure includes any MOA service that if compromised would pose a great risk or cause significant impact to Municipal operations and/or resources.*
- 04/11/2023: At 2 pm, Dahl emails the posted policy and an intranet page link to himself, from his MOA email address to his MOA email address.
- 04/11/2023: Graham, who filed the original election complaint, signed in at the MOA Election Center at 2:34 pm and subsequently filed a handwritten document on behalf of herself and two other election observers for the Trueblood campaign, John Henry and Daniel Smith. The header on the document, which would go to the Election Commission, read “Election Commission – Failure to Comply with Law or Alleged Illegal Election Practices”. The document quoted, word for word, the internal OIT policy that had been posted 66 minutes earlier on OIT’s internal MOA intranet page, whose existence was only known to three MOA employees at that time, and that was not publicly posted or accessible. The election challenge document stated that “It is completely possible that the USB device is depositing or altering data, intentionally or unintendedly, not simply retrieving data, thereby nullifying the results of the election”.
- 04/11/2023: At 2:37 pm, Dahl emails the policy and intranet link to Graham, who had filed the 04/06/2023 election complaint, and who subsequently filed the election challenge on 04/11/2023.
- 04/12/2023: Director Dahl is captured on the security video cameras at the MOA Election Center picking up one of the election observer complainants, John Henry, at 11:27 am, and then dropping him off at the Election Center at 1:12 pm.
- 04/14/2023: At 11:31 am, Dahl emails information to Graham regarding an item for the 04/18/2023 Special Assembly Meeting agenda, AO 2023-45, which would recognize the decision-making authority of the assembly with respect to uncodified mayoral



directives, policies, and procedures, and other uncodified policies and administrative practices as applied to the legislative branch.

- 04/14/2023: Graham files another election complaint that references AO 2023-45 and states that the ordinance, “written by Christopher Constant – a candidate in the current election – is a direct response to the appeal dated Apr. 11. It changes the processes and procedures of an election during the middle of an election.”
- 04/16/2023: MOA Election Coordinator, Jamie Heinz responds, via email, to Graham’s 04/14/23 complaint. The subject line is “2<sup>nd</sup> Appeal Re. Thumb Drive” –  
*“This email is in response to your second appeal regarding the thumb drive, which was filed on Friday, April 14<sup>th</sup>. In this second appeal, you note AO 2023-45 as item 5.A. on the Special Meeting Agenda for Tuesday, April 18<sup>th</sup>. Please note that the items up for public hearing at the April 18<sup>th</sup> meeting were introduced at the April 7<sup>th</sup> Special Meeting. Attached, you will find an email stating that the agenda deadline for items to be submitted to the Clerk’s Office for inclusion in the April 7<sup>th</sup> Special Meeting was noon on Wednesday, April 5<sup>th</sup>. Also attached you will find an email, sent out at 10:57 a.m. on Thursday, April 6<sup>th</sup>, which provides the entire packet of materials for the April 7<sup>th</sup> Special Meeting. You will see included in the packet, item 6.A., AO 2023-45.*

*This ordinance was in the works and submitted to the Clerk’s Office before noon on Wednesday, April 5<sup>th</sup> which is before your initial complaint was submitted the afternoon of April 6<sup>th</sup> and the timeline is purely coincidence.”*

- 04/20/2023: The Anchorage Election Commission held their Public Session of Canvass and Adoption of the Election Canvass Report. Agenda item 5.C.a, under New Business, was *The Election Commission – Failure to Comply with Law or Alleged Illegal Election Practices* re MOA ITD USB POLICY STATEMENT. This was the election challenge filed by Graham, Henry, and Smith. After hearing from Graham and Heinz, the Commission votes to deny the election challenge.
- 04/26/2023: A constituent, who had listened to the 04/20/2023 Commission meeting, contacted the Ombudsman with their concerns regarding the actions of Dahl related to the development and posting of the OIT USB policy on the OIT intranet on April 11th.

## ANALYSIS AND CONCLUSIONS

During his investigation of this matter, the Ombudsman considered all of the documents and records that were available to him, the statements of witnesses and OIT employees and former employees, his personal observations of Dahl at the MOA Election Center during the April 5, 2022 Municipal Election ballot tabulation processing and the May 26, 2022 Logic and Accuracy Testing for the June 21, 2022 Special Election, and the timeline of events, before making a determination. The key factor for the Ombudsman was the timing of events, which supports the conclusion that Dahl initiated and directed the revision and posting of the OIT USB policy to provide support for a challenge of the April 4, 2023 Municipal election that was filed by election observers with the Trueblood campaign.



Multiple governmental, business, and private organizations have implemented USB drive policies like the USB policy developed and posted on the OIT intranet page on April 11<sup>th</sup> - the Ombudsman acknowledges that many organizations consider such policies to be a best practice. However, documents show that Dahl restarted the conversation regarding the draft OIT USB policy on the morning of April 11<sup>th</sup>, after Graham had submitted an election complaint on April 6<sup>th</sup> that referenced the use of USB drives. The documents also show that Dahl had requested that the policy be revised to include a reference to thumb drives and the exchange of information on critical infrastructure, and that the policy be posted on the OIT intranet that same day – the day that Graham subsequently filed an election complaint that cited, word for word, the OIT policy that only three MOA employees were aware of, and that was not available to the public or publicly posted. Documents also show that Dahl emailed the policy to Graham on April 11<sup>th</sup>, the day that her election complaint was filed.

On April 14<sup>th</sup>, Dahl emailed Graham to inform her regarding an ordinance, 2023-45, that was being heard at a Special Assembly Meeting on April 18<sup>th</sup>. The same day, April 14<sup>th</sup>, Graham filed an election challenge that claimed that AO 2023-45 had been introduced in response to her April 6<sup>th</sup> election challenge, although the draft ordinance had been submitted to the Clerk's Office on April 5<sup>th</sup>. Dahl's emails to Graham demonstrate that he was acquainted with Graham and was feeding her information to assist her in formulating challenges to the April 4<sup>th</sup> Municipal election. Video surveillance recordings from the Election Center that show Dahl picking up and dropping off John Henry at the Election Center on April 12<sup>th</sup>, demonstrate that he is acquainted with Henry, who, along with Graham and Daniel Smith, submitted the April 11<sup>th</sup> election challenge on behalf of the Trueblood campaign.

Any reasonable person can connect the dots – there is no way to dismiss the timeline of events as merely coincidental – the timeline and supporting documents demonstrate that Dahl was acquainted with at least two of the three Trueblood election observers who filed the election challenge on April 11<sup>th</sup>, and that the dormant OIT USB policy development discussion was restarted on April 11<sup>th</sup> at the instigation of Dahl, who directed that the final policy be posted on the OIT intranet page that same day. The timeline, and Dahl's email to Graham demonstrate that Dahl was directing the development and posting of the policy to provide support for the impending election challenge. As an executive with the Municipality, Dahl has an obligation to remain politically neutral in the performance of his official duties – an obligation that he failed to meet multiple times regarding Graham's election challenges.

The Ombudsman's personal observations of Dahl's actions at the Election Center in 2022 demonstrate that Dahl has trouble separating his personal political beliefs from his role as an executive with the Municipality of Anchorage – the inability of any Municipal executive to separate their personal political beliefs from their professional role is problematic for the Municipality and Mayoral Administration that they serve.

AMC 28.80.015.B states that "All ballot tabulation processing using a software application shall be under the supervision of the municipal clerk and observance by at least one of the following selected by the municipal clerk:

## Attachment O

1. Internal Auditor or designee.
2. IT director or designee.
3. Municipal ombudsman or designee.”

The Clerk invited the Internal Auditor, IT Director, and Ombudsman to observe the ballot tabulation processing at the Election Center on the evening of April 5, 2022. The Internal Auditor and Ombudsman arrived and joined the Clerk and elections staff in front of the election computers – the IT Director arrived and effusively greeted the election observers and joined them, rather than sitting with the other official Municipal ballot tabulation observers. The Director discussed the election with the election observers, while representing the Municipality as an official ballot tabulation observer. The Ombudsman was troubled by the actions of the Director and later that evening expressed his concerns to the Clerk and Election Administrator – the Ombudsman believed that it was inappropriate for the Director to be discussing the election and expressing partisan political opinions to election observers, while serving as an official Municipal ballot tabulation observer. The Ombudsman discussed filing a complaint with the Ethics Board but decided not to file.

The Ombudsman and Internal Auditor were invited to observe the May 26<sup>th</sup>, 2022 Logic and Accuracy Testing at the MOA Election Center, for the June 21, 2022 Special Election. Shortly after they arrived, Dahl arrived – he was present as a member of the public and was not representing the MOA. Dahl was provided with a yellow lanyard to wear around his neck – yellow signified that he was a member of the public and that he had to stay on the “yellow brick road”, a pathway outlined in yellow that circles the core area of the Election Center. Persons with yellow lanyards must stay on the outlined pathway. Dahl kept crossing the pathway’s boundary, entering areas of the Election Center that were off-limits to persons with yellow lanyards. The Clerk warned Dahl several times to stay on the pathway – when he thought that the Clerk was not looking, Dahl walked over to the reception desk, took off his yellow lanyard, reached across the reception desk to get a different colored lanyard, and put that lanyard around his neck. That lanyard provided greater access to areas within the Election Center. The Clerk observed Dahl’s actions and told him that he could not assign himself a different color of lanyard – he was present as a member of the public and he needed to wear a yellow lanyard.

An executive with the MOA told the Ombudsman that Dahl had commented to him, at work, that the April 2022 Municipal election had been “rigged”. Dahl’s comments, actions at the election center, and his actions regarding the April 11<sup>th</sup> development and posting of the OIT USB policy demonstrate a pattern of behavior that is troubling and that needs to be addressed – his actions and inability to separate his personal political views from his role as an executive with the MOA has damaged the reputation of OIT and has eroded the trust of MOA employees in the ability of OIT to be impartial and neutral. Given the wide-ranging access that OIT staff has to MOA facilities and systems, it is imperative that MOA employees have confidence in OIT’s ability to be impartial and neutral – the actions of Dahl as OIT Director have negatively impacted the hardworking, dedicated OIT employees who come to work everyday doing the best they can to keep the MOA functioning smoothly – they, and the public deserve better.



Based on the available evidence and the actions of the OIT Director, the Ombudsman finds this complaint regarding the Municipality of Anchorage, Office of Information Technology, Director to be **JUSTIFIED**.

**Based on the investigation of this case, the Municipal Ombudsman recommends:**

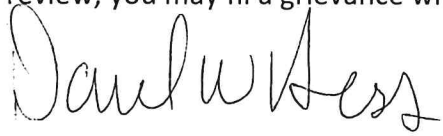
- That the Administration terminate Marc Dahl's employment with the Municipality of Anchorage. His actions have damaged the reputation of the Municipality's Office of Information Technology and has undermined the trust of other Municipal departments, agencies, and employees that is necessary for the department to accomplish its mission. His actions have also damaged the reputations of the hardworking, dedicated OIT personnel who were simply following the directives of their department director. ***The Administration did not provide a response to this recommendation.***
- That Anchorage Municipal Code be revised to apply the restrictions regarding participation in Municipal elections that apply to the Ombudsman's Office to the directors of all Municipal departments, utilities, and enterprises. ***The Administration did not provide a response to this recommendation.***
- That the Assembly and Administration work together to develop and implement in Municipal Code penalties for tampering or attempting to tamper with Municipal elections. As a Home Rule Municipality that encompasses 40% of the state's population, the Municipality should not have to rely on state statutes regarding tampering or attempting to tamper with our election. ***The Administration responded – "The Administration will work with the Assembly to develop and implement Municipal Code addressing tampering or attempting to tamper with Municipal elections."***
- That the Administration implement and require annual ethics training for all Municipal employees. The company that currently provides our mandatory annual online training has an optional ethics module. ***The Administration responded – "The Administration recommends that all Municipal employees – from both the Executive Branch/Administration and Legislative Branch/Clerk's Office/Assembly – receive annual ethics training, to include proper interaction between Municipal employees who work on critical election infrastructure and the public."***

The Ombudsman reasonably believes that there may have been a violation of state election statutes and will be forwarding a copy of the Final Investigative Report to the State of Alaska, Office of Special Prosecutions.

The Administration was provided with a copy of the preliminary investigative report on July 25, 2023. The Administration's written response was received on August 17, 2023. Their responses to the Ombudsman's recommendations were incorporated into the final report, and their comments are appended to the report. The Administration, at the request of the Ombudsman, provided a copy of the preliminary report to Dahl on July 31, 2023, to allow him an opportunity to provide comments – he has not submitted any comments regarding the preliminary report.

**Based on these findings and these recommendations, this case is closed.**

If you object to the Ombudsman's decision to decline, discontinue, or close this investigation or review, you may file a grievance with the Ombudsman as specified in A.M.C. 2.60.165.

A handwritten signature in black ink that reads "Darrel W. Hess". The signature is written in a cursive style with a large initial "D".

Darrel W. Hess  
Municipal Ombudsman



**MUNICIPALITY OF ANCHORAGE**  
**MAYOR DAVE BRONSON**

---

**DATE:** August 17, 2023

**TO:** Darrel W. Hess, Ombudsman

**FROM:** Mario Bird, Chief of Staff *MLB*  
Kent Kohlhase, Municipal Manager *KK*

**SUBJECT:** Preliminary Investigative Report Concerning Ombudsman Complaint 2023-0550

---

Please accept this as the Administration's response to the draft Ombudsman's report 2023-0550 dated July 24, 2023. The Administration is supportive of the process and would like to recognize that the Administration and its employees have cooperated to the fullest extent asked by the Ombudsman. The Administration agrees that Election integrity is critical to the legitimacy of the government and the public trust.

After reviewing the Ombudsman's preliminary report, the Administration appreciates the level of detail that went into the process. Please see our comments and areas of identified response below.

1. The Director of the Municipality of Anchorage's Office of Information Technology (OIT) did not follow Policy & Procedure 1-1, specifically regarding the publication of the revised OIT policy that appeared on the OIT intranet page on or about April 11, 2023. Though the process used by the IT Director was improper, the Administration will introduce an updated MOA-wide policy that accomplishes many of the OIT policy goals, including protection of MOA OIT assets, especially screening for malware that can enter an MOA system through a thumb drive or other standalone device.
2. The Administration recommends that all Municipal employees – from both the Executive Branch/Administration and Legislative Branch/Clerk's Office/Assembly – receive annual ethics training, to include proper interaction between Municipal employees who work on critical election infrastructure and the public.
3. The Administration will introduce a personnel policy or code change which applies to Municipal employees working on critical infrastructure during elections, specifically addressing appropriate limitations on communication between such employees and public or partisan vote observers.

4. The Administration will work with the Assembly to develop and implement Municipal Code addressing tampering or attempting to tamper with Municipal elections.
5. The Administration respectfully requests that the final report adhere to AMC 2.60.145 by removing any identifying information for municipal witnesses (excluding the subject employee).
6. Per the Ombudsman's request, Mr. Marc Dahl was provided a copy of your preliminary report on July 31, 2023, so that he may also provide comments. We ask that the Ombudsman's office please communicate directly with Mr. Dahl going forward. Please feel free to directly contact Mr. Dahl at: [dahlsons@hotmail.com](mailto:dahlsons@hotmail.com), should you wish to do so.

Thank you for receiving the comments of the Administration. It is respectfully requested that these comments be attached to the final report consistent with the Municipal Code. Here ends the comments of the Administration.





## Anchorage Assembly Leadership

August 18, 2023

Mayor Dave Bronson  
632 W. 6<sup>th</sup> Ave., Suite 850  
Anchorage, AK 99501

Sent via email only

Re: Public records request— *April 11 Election Complaint and Creation of ITD Policy Statement Regarding Removable Storage Devices*

Mayor Bronson:

As you know the Assembly recently held a Worksession on July 21, 2023 to address the creation and internal posting of an ITD Policy Statement and the apparent role it played in an April 11, 2023 election complaint filed by Ms. Sami Graham. We regret that you were unable to attend.

Prior to the Worksession, Assembly Chair Constant submitted a public records request to the Department of Law requesting, among other things, communications pertaining to the development of this policy statement. In response, we received more than 130 pages of responsive documents. Of these documents, several particularly relevant documents had been redacted. Specifically:

- An email dtd January 10, 2023 from Mark Merchant to Marc Dahl, Subject “FW: Policy - 28-10” and its attachment P&P 28-10, Subject: Protection of Personal or Confidential Information”
- An email dtd January 18, 2023 from Mark Merchant to Marc Dahl, Subject “Draft Round 2” and its attachment, P&P 28-41, Subject: Miminimum security erequiements for internet and system connectivity.
- An email dtd April 11, 2023, sent at 9:30am, from Mark Merchant to Marc Dahl, Subject “RE: Draft Round 2”
- An email dtd April 11, 2023, sent at 10:09am from Marc Dahl to Mark Merchant, Subject “RE: Draft Round 2”
- An email dtd April 11, 2023, sent at 10:14am, from Mark Merchant to Marc Dahl, Subject “RE: Draft Round 2”
- An email dtd April 11, 2023, sent at 10:42am from Marc Dahl to Mark Merchant, Subject “RE: Draft Round 2”

It is our understanding that the Department of Law did not have time to consult with the IT Department prior to providing these documents to the Chair, and they made

these redactions out of an abundance of caution, and not, necessarily, because your Administration wished to unequivocally assert the deliberative process privilege.

As discussed at the July 21<sup>st</sup> Worksession, these emails immediately preceded the posting of an ITD Policy Statement “Regarding Removable Storage Devices” to the Municipality’s internal sharepoint site at approximately 1:318 p.m on April 11<sup>th</sup>. The text of that policy statement appears to have been emailed by Mr. Dahl to Ms. Graham at 2:37 p.m. who, in turn, at 3:47p.m, filed a complaint in the April 4, 2023 regular municipal election. This complaint alleged a “clear violation of the MOA ITD USB Policy Statement” by the Clerk’s Office and that it was “completely possible that the USB Device[used by elections officials to retrieve data from municipal voting equipment was] depositing or altering data, intentionally or unintentionally, not simply retrieving data, thereby nullifying the results of the election.”

Chief of Staff Mario Bird addressed the creation of this ITD Policy Statement at our Worksession, describing your office as not having “any knowledge of the development of this policy, unless and until it became part of the public record and it was reported upon. . . we were unaware of the ITD policy statement until the scrutiny that was levied by the media.”<sup>1</sup> Mr. Bird also explained the Administration’s established process for creation of Municipal Policy, which is found in Policy & Procedure 1-1, stating that “Policies and Procedure that run through the Administration are required to go through a process that begins with OMB [Office of Management and Budget] and involves all the relevant departments and then at the conclusion of that discussion, OMB finalizes what that last policy should look like, and the Mayor signs off. . . So, when this came to our attention, one of the first things our OMB Director said, ‘if this is accurate, what’s being reported in the paper, this is not a policy that went through our policy for policies,’ if you’ll forgive the term.”<sup>2</sup>

In light of these facts, the Assembly Leadership does not see any appropriate foundation for the assertion of the deliberative process privilege and requests your office release the previously redacted emails as public records under Alaska Statute 40.25.110.

### The Deliberative Process Privilege

The deliberative process privilege “protects internal communications ‘which reflect advisory opinions, recommendations, and deliberations comprising part of the process by which governmental decisions and policies are formulated.’”<sup>3</sup> The basis of

---

<sup>1</sup> Worksession re April 11 Election Complaint and Creation of ITD Policy re Removable Storage Devices available at <https://www.youtube.com/live/yrejN64cMJM> at 14:02.

<sup>2</sup> *Id.* at 14:50.

<sup>3</sup> 1992 Inf. Op Att’y Gen (Nov. 5; 221-92-0553)(citing *Dowd v. Calabrese*, 101 F.R.D. 427, 430 (D.C. Cir. 1984)). While the Alaska Supreme Court has issued several significant opinions governing the application of the deliberative process privilege, the bulk of precedent has been generated by the federal courts. As a result, both the state judiciary and Attorney-General look to this body of precedent in determining how



the privilege lies in the government's important interest in protecting the mental processes of its decisionmakers from unreasonable interference. To determine whether disclosure would interfere with that process, courts have required those asserting the privilege "show as a threshold matter that the communication is both 'predecisional' and 'deliberative.'"<sup>4</sup>

### The Predecisional Element

The predecisional element, as the term implies, requires the communication be made "before the deliberative process was completed."<sup>5</sup> Implicit in this requirement, is that a deliberative process be actually initiated at some point. This prerequisite is reflected in the relevant Alaskan caselaw governing the privilege, all of which involve communications addressing specific issues and being sent to, or within the office of, the relevant decisionmaker.<sup>6</sup> In contrast, these redacted records relate to a policy statement which was created, published, and shared with public prior to you even being made aware of its existence. Far from being "prepared in order to assist [you] in arriving at [a] decision"<sup>7</sup>, these communications and documents appear to have been either inadvertently or deliberately withheld from you, your office, and OMB. In light of these facts, these records would be better characterized "extra-decisional" as opposed to "predecisional," and a court would be unlikely to stretch the predecisional element so far as to encompass them.

### The Deliberative Element

The deliberative element, requires the communication "reflect a 'give-and-take' of the decisionmaking process and contain opinions, recommendations, or advice about agency policies. Purely factual material is not protected unless the selection process or presentation would reveal the decisionmaking process, or if the facts are inextricably intertwined with that process."<sup>8</sup> While Alaska courts have yet to embrace a strict test for determining the deliberative nature of policy drafts, both the Second and DC Circuits have explicitly required the such a disputed record be "related to the process by which policies are formulated."<sup>9</sup> More recently the D.C. Circuit Court of Appeals has imposed an upfront burden on any "agency invoking the deliberative-process privilege [to]. . . 'establish what deliberative process is involved, and the role played by the documents

---

and when the deliberative process privilege may apply. *See id.*; *see also Griswold v. Homer City Council*, 428 P.3d 180, 187 (2018).

<sup>4</sup> *Gwich'in Steering Committee v. State, Office of the Governor*, 10 P.3d 572, 579 (2000).

<sup>5</sup> *Griswold supra* note 3 at 188.

<sup>6</sup> *See id.* at 581 (discussing the application of the privilege to documents sent to the Office of the Governor and internal emails within the Office of the Governor); *see also Griswold supra* note 3 at 188-89 (discussing the application of the privilege to advice and draft documents sent from the advising attorney to the Homer Board of Adjustment); *see also Fuller v. City of Homer*, 75 P.3d 1059, 1060 (Alaska 2003) (discussing the application of the privilege to communications from Department Heads to the city manager).

<sup>7</sup> *Grand Cent. Partnership, Inc. v. Cuomo*, 166 F.3d 473, 482 (2d Cir. 1999).

<sup>8</sup> *Gwich'in supra* note 4 at 583.

<sup>9</sup> *Hopkins v. United States Dep't of housing and Urban Development*, 929 F.2d 81, 84 (2d Cir. 1991).

in issue in the course of that process.”<sup>10</sup> Here, your IT department bypassed your “process by which policies are formulated”<sup>11</sup> as established in P&P 1-1, and, at present, there appears to be no other legitimate process in which these draft documents played any role. In the analogous case of *Bonner v. CIA*, the D.C. District Court ruled that a draft CIA report was not exempt from disclosure under the Freedom of Information Act precisely because the government “fail[ed] to identify any agency decision-making process in connection with which the document was created.” Simply arguing that these were communications were policy drafts is not enough, these documents must have been part of your deliberative process to claim the privilege.

### Public Interest

Finally, even assuming, without conceding, these documents actually do meet the threshold to claim the deliberative process privilege, you must still balance what interest your Administration has in maintaining this secrecy, with the public’s significant interest in transparency.<sup>12</sup> Given that the very purpose of the deliberative process privilege is to “protect the executive’s decisionmaking process, its consultative functions, and the quality of its decisions,”<sup>13</sup> we are confident you will agree that your Administration cannot honestly claim a legitimate interest in protecting the documents at issue when they appear to be created for the benefit of Ms. Graham, and not your office, nor the Municipality.

### Conclusion

In short, the evidence we have seen indicates authors of these emails worked expediently and not deliberatively; they engaged in an improvisation, not a process; and they produced an illegitimate and invalid policy statement that served only to assist a private citizen’s attempt to call a valid municipal election into question, and not to assist you in protecting the Municipality’s technical infrastructure. Based on the facts presented to the Assembly and the body of relevant caselaw, we fail to see a rational argument for the application of deliberative process privilege to the emails preceding the publication of the ITD Policy Statement at issue. We are confident any court will agree. In the interest of transparency and confidence in our government, we respectfully request you release the previously redacted documents by 12:00 p.m., August 22, 2023.

---

<sup>10</sup> *Citizens for Resp. & Ethics in Washington v. United States Dep’t of Just.*, 45 F.4th 963, 973 (D.C. Cir. 2022) (quoting *Senate of the Commonwealth of Puerto Rico ex rel. Judiciary Comm. v. Dep’t of Just.*, 823 F.2d 574, 585–86 (D.C. Cir. 1987)).

<sup>11</sup> *Hopkins supra* note 9.

<sup>12</sup> See *Gwich’in, supra* note 4 at 583-84.

<sup>13</sup> *Id.* at 578 (citing *Capital Info. Group v. State, Office of the Governor*, 923 P.2d 29, 33(1996).

Attachment P

Thank you for your attention to this matter. If you have any questions, we would be happy to discuss.

Sincerely,



Christopher Constant, Assembly Chair



Meg Zaletel, Assembly Vice Chair

Cc: Anne Helzer-Municipal Attorney  
Kent Kohlhasse - Municipal Manager  
Mario Bird - Chief of Staff  
Assembly members



## Anchorage Assembly Leadership

September 5, 2023

Mayor Dave Bronson  
632 W. 6<sup>th</sup> Ave., Suite 850  
Anchorage, AK 99501  
[dave.bronson@anchorageak.gov](mailto:dave.bronson@anchorageak.gov)

Sent via email only

Re: Request for documents concerning the 2022 and 2023 regular elections

Dear Mayor Bronson:

As you know, the Ombudsman has recently published a report regarding his investigation into the circumstances surrounding an election complaint filed by election observer Sami Graham on April 11, 2023 and an internal policy statement created by your administration which was used as the basis of the complaint. As the elected leadership for, and long-serving members of, the Assembly, we take the Ombudsman's findings and recommendations very seriously. Per Article IV of the Anchorage Charter, the Anchorage Assembly serves as the judge of Anchorage Elections, and per Article XI the Assembly is charged with establishing the election procedures by ordinance. Bound by the charter, we have a duty to understand the circumstances described in the Municipal Ombudsman's investigation and, as appropriate, propose amendments to the code to protect future municipal elections from tampering. We know your Administration was given the opportunity to respond to the Ombudsman's report prior to its finalization, and we were pleased to see your stated desire to work with the Assembly to preserve the security of our elections as expressed through your Chief of Staff, Mario Bird.

That said, it has not been lost on us that, thus far, the only people to have been implicated in this matter, Ms. Graham and Mr. Dahl, were both your political appointees: the former having served as one of your first chiefs of staff, and the latter as your current IT Director since 2021. Nor has it been lost on us that the complaints filed by Ms. Graham regarding the 2023 regular election bear a striking resemblance to questions you posed in a records request letter to the Municipal Clerk on April 29, 2022 regarding the 2022 regular election. It is also worth noting that, when you sent this letter, you chose to Cc Mr. Dahl.

In questioning the legitimacy of the 2022 election, your letter cited the "widespread questions and concerns related to the voting process" your office purportedly received. Given your expressed commitment to "create and foster an environment of additional trust and integrity for future Municipal Elections" the Assembly Leadership hereby requests you produce the following documents as public records under Alaska Statute 40.25.110 and Anchorage Municipal Code Chapter 3.90:

- Records of any communications to, from, or between current and former employees of your office discussing complaints or allegations of misconduct in either the 2022 or 2023 Regular Election; and

**Attachment Q**

Mayor Dave Bronson

September 5, 2023

Page 2 of 3

- Records of any communications to, from, or between current or former employees of your office or any other current or former municipal employee and Ms. Sami Graham.

In conducting a search of electronic records we request you use the following parameters: Records between April 1, 2022 and May 1, 2023 containing any of the following keywords:

- “alaskansam@yahoo.com”
- “alaskangraham@yahoo.com”
- “election”
- “dominion”
- “overturn”
- “rigged”
- “Leung”
- “BallotTrax”
- “ballot”
- “thumb drive”
- “USB”

For the purposes of this request please construe the term “your office” broadly to include all those staff working directly for the Mayor, whether as contract employees or as municipal employees. It includes, but is not limited to, your chief of staff, municipal manager and their respective deputies and administrative staff.

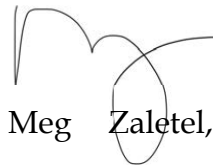
To the extent the Administration believes any information contained within these documents is privileged, please precisely redact the information you believe to be privileged, and denote the specific nature of the privilege being asserted, either on the document itself or on an accompanying redaction log. At a minimum the log must identify the sender, the recipient, and the subject of the communication over which a privilege is being asserted. This method of redaction is in keeping with both best legal practices and the spirit of the caselaw regarding privileged information.<sup>1</sup>

We request that you please provide any responsive records of correspondence to or from Ms. Graham or Mr. Dahl to us either physically or via email no later than 5:00p.m. Thursday, September 7, 2023 and the remainder of the requested records no later than 12:01p.m. Tuesday, September 26, 2023.

Sincerely,



Christopher Constant, Assembly Chair  
Chair



Meg Zaletel, Assembly Vice

---

<sup>1</sup> See *Doe v. Alaska Superior Court, Third Judicial Dist.*, 721 P.2d 617, 626 (Alaska 1986).

**Attachment Q**

Mayor Dave Bronson

September 5, 2023

Page **3** of **3**

Cc: Anne Helzer–Municipal Attorney  
Kent Kohlase – Municipal Manager  
Mario Bird – Chief of Staff  
Phillippe Brice – Acting IT Director  
Assembly members

ADVERTISEMENT

# Bronson administration currently taking no action against IT Director involved in election complaint



Bronson Administration taking no action at this time against IT Director involved in election complaint

By [Steve Kirch](#)

Published: Sep. 8, 2023 at 7:09 PM AKDT



ANCHORAGE, Alaska (KTUU) - Anchorage Mayor Dave Bronson's administration is taking no action at this time against a member of his team who was implicated in a plan to possibly overturn some results of the April 4 municipal election.

This comes as ombudsman Darrel Hess's final investigation report recommended the administration terminate the employment of information and technology director Marc Dahl for his involvement in the matter.

When asked Friday about Dahl, municipal attorney Anne Helzer told assembly members at a work session regarding the ombudsman's investigative report that Bronson had a discussion with Dahl about possibly submitting a resignation, and was anticipating an answer by the end of the day.

An official with the Bronson administration said at this time Dahl is still on administrative leave, and it is unclear if the administration will take any action in the future.

ADVERTISEMENT





When reviewing the ombudsman’s report, Hess told assembly members there was clearly a coordinated effort between Dahl and the mayor’s former chief of staff Sami Graham to overturn election results through the creation of an unofficial IT department policy.

According to documents, Graham filed a complaint on April 6 that election staff was using USB drives to transfer election data from voting tabulation machines to municipal-owned computers. Graham said she was concerned the USB drives could “intentionally” or “unintentionally” alter election results.

On April 11, the municipality’s chief information security officer Mark Merchant emailed and coordinated with Dahl on crafting a new Information Technology Department policy stating “personnel must not insert any unauthorized USB device into any piece of MOA owned equipment without authorization from the information technology department.”

Merchant then emailed and instructed system analyst Heather Holland to create a link to the informal policy on a non-public website used internally by municipal employees. Dahl then emailed Graham a link to the new policy, which she then used to support her initial complaint.

ADVERTISEMENT

“It’s difficult to make any other conclusion than to follow the record where the records lead us. Because it looks like there was coordination between a municipal staff member and a former municipal staff member to make a complaint that looked like it could overturn an election. That is an unacceptable abuse of our electoral process,” Assembly chair Chris Constant said.

Bronson’s current chief of staff Mario Bird has stated the mayor was unaware of the events surrounding the election complaint and the policy.

Bronson said in May 2023, he was informed of Dahl’s involvement in a complaint regarding the April 2023 election. At that time, he was placed on leave.

However, in a statement Friday, Bronson said, “Since then, the Ombudsman’s investigation has been completed, and the final report has been published. I have had time to review it thoroughly and I do not see any evidence that Mr. Dahl conducted any illegal behavior. In fact, the Ombudsman’s report outlines the policy Mr. Dahl attempted to implement is common practice by governmental organizations, businesses, and private organizations.”

Bronson added, “However, it is clear that the MOA policy to implement new processes and procedures was not followed by Mr. Dahl. The issue is not about the policy Mr. Dahl attempted to implement; it is the timing in which the events occurred, and the lack of process followed that is in question.”

When asked if the administration expects Dahl to resign, an official said she does not have an answer at this time.

[How to watch Alaska’s News Source your way with our family of streaming apps](#)

Copyright 2023 KTUU. All rights reserved.

**Heart Surgeon Begs Americans: “Stop Doing This To Your Blueberries”**

Dr. Gundry has released an informative free video showcasing exactly which foods you may need to avoid.

Gundry MD | Sponsored

Learn More

**If you have a mouse, this game will keep you up all night. No Install. Play for free.**

Combat Siege | Sponsored

**Breakthrough Device Gives Hope To Seniors Suffering From Back Pain**

Health Insight Journal | Sponsored

Learn More

