Board of County Commissioners Agenda Request

5B
Agenda Item #

Requested Meeting Date: May 28, 2024

Title of Item: Approve General Operations Policy Updates

☑ REGULAR AGENDA	**Action Requested:**	☐ Direction Requested
☐ CONSENT AGENDA	☑ Approve/Deny Motion	☐ Discussion Item
☐ INFORMATION ONLY	☐ Adopt Resolution (attach draft)	☐ Hold Public Hearing*
	**provide copy of hearing notice that was published*	

Submitted by: Jessica Seibert	**Department:** Administration
Presenter (Name and Title): Jessica Seibert, County Administrator	**Estimated Time Needed:** 3 Min.

Summary of Issue:

Several changes have been made to the current Meal Reimbursement section of the General Operations Policy based on feedback from payroll and accounting staff. Feedback from department heads has also been incorporated. Changes are noted in red on the attached policy.

Section 3(k) of the General Operations Policy has been developed to address Data Security Breach Protocols.

Alternatives, Options, Effects on Others/Comments:

Recommended Action/Motion:
Approve General Operations Policy Updates.

Financial Impact:
Is there a cost associated with this request? ☐ *Yes* ☑ *No*
What is the total cost, with tax and shipping? $
Is this budgeted? ☐ *Yes* ☐ *No* *Please Explain:*

Legally binding agreements must have County Attorney approval prior to submission.

P. Meal Reimbursement

1. Purpose: ~~T~~To define the meal reimbursement procedures for County employees, elected officials, and authorized representatives for expenses incurred while conducting business on behalf of Aitkin County as required by the County.

2. Aitkin County will provide reimbursements for meal expenses when such expenses are necessarily incurred while conducting County business. The Department Head or Supervisor must approve all requests prior to incurring reimbursable expense.

a) The Department Head or Supervisor must approve requests by signing Day Meal or Overnight Vouchers as follows:

Day Meals: Complete Day Meal Reimbursement Form and attach a detailed receipt showing items purchased (a receipt showing only the total is not sufficient) OR a detailed Declaration of Expenses Form.

Overnight Meals: Complete a Voucher and attach a detailed receipt showing items purchased (a receipt showing only the total is not sufficient).

~~3.~~ The actual cost of meals, not to exceed $57.00 per day, while traveling outside of the County will be reimbursed. The following daily amounts shall be followed:

Breakfast: $13.00 Lunch: $17.00 Dinner: $27.00

4.~~3.~~ Conditions

a. Employees who meet the eligibility requirements for two (2) or more consecutive meals, shall be reimbursed for the actual cost of the meals up to combined maximum reimbursement amount.

b. Reimbursements may be claimed by the individual if they depart from work location in an assigned travel status before 6:00 a.m. or if the individual is away from home overnight.

c. Individuals may claim reimbursement if they are not within the County boundaries during the regular scheduled lunch period.

Formatted: Indent: Left: 1.15", No bullets or numbering

Formatted: Underline

Formatted: Indent: Left: 1.13", Hanging: 0.03", No bullets or numbering, Tab stops: 1", Left + Not at

Formatted: Indent: Left: 1.15", No bullets or numbering

d. Reimbursement may be claimed by the individual if they are away from their normal work location in a travel status overnight or requirement to remain in a travel status until after 7 p.m.

e. The Department Head must authorize meetings with a meal charge in excess of the approved meal allowance.

f. When meals are part of a tuition or registration fee, no additional reimbursement request for such meals can be claimed.

g. Expenses of alcoholic beverages are not reimbursable.

h. Tips are not reimbursable. If a tip or auto gratuity service fee is automatically charged by the restaurant, it will be reimbursed up to 20% of the meal allowance.

i. The reimbursement for meals, lodging, parking, and other related County expenses will occur only upon submittal of receipts. Pursuant to federal law, meal reimbursement without overnight lodging will be included as income tax withholding and FICA deduction. Reimbursement for out of state travel shall be made at the Federal CONUS rate at the time of travel.

j. If meals are included as part of a conference, seminar fee, or airline ticket and or not separately identified, they are not taxable income.

k. Day Meals cannot be charged to an Elan card.

l. Each employee must pay for their own meal and submit a separate itemized receipt. More than one employee cannot be included on the same receipt.

Q. Conference/Seminar Request

1. Aitkin County employees must keep up to date with changes being made outside the county which affect the way county business is performed. It is also the intent of Aitkin County to encourage development of its staff to the fullest extent possible. Two areas that are used for this are "required" and "discretionary" training.

To be added to General Operations Policy -

Section 3. Information Systems and Technology

Item K. Data Security Breach Protocol

APPENDIX E
DATA SECURITY BREACH PROTOCOL

Part 1. Purpose.

This protocol is intended to assist Aitkin County in implementing the requirements of Minn. Stat. § 13.055 that is intended to provide timely and appropriate notice to individuals who are affected by a breach of the security of their private or confidential data. All employees must immediately report known or potential breaches of security to the responsible authority as identified in the Aitkin County Data Practices Policy and their supervisor. The County Attorney's Office in consultation with the affected department or office or Information Technology personnel as appropriate shall determine whether notice of the potential breach is required and if so how the notice will be provided. This protocol shall be integrated with the Aitkin County Information Systems and Technology section of the Aitkin County General Operations Policy of which is included and incorporated in the event a potential data breach or data breach involves electronic related data, resources or components.

Part 2. Definitions. Minn. Stat. 13.055, Subd. 1 (in part)

Subpart A. Potential Data Security Breach. A situation or incident that provides a reasonable basis to believe not public data may have been compromised or accessed for a purpose not authorized by law or by a person or entity not authorized by law to have access to such data.

Subpart B. Breach of the security of the data. Breach of the security of the data means the unauthorized acquisition of data maintained by the county in any medium that compromises the security and classification of the data, but not including the good faith acquisition by an employee, contractor or agent of the county if not provided to an unauthorized person.

Subpart C. Contact Information. Contact information means either name and mailing address or name and e-mail address for each individual who is the subject of data maintained by the county.

Subpart D. Unauthorized acquisition. Unauthorized acquisition means a person has obtained government data without the informed consent of the individuals who are the subjects of the data or lacks statutory or other legal authority and with the intent to use the data for non-governmental purposes.

Subpart E. Unauthorized person. Unauthorized person means any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data.

Part 3. Guidelines

Subpart A. Reporting a Potential Breach. Any employee who knows of or reasonably believes breach of the security of private or confidential data may have occurred must immediately report to his or her supervisor and the county's responsible authority. (R.A.)

The report should include the date and time of the report, when the breach occurred (if known); the type of data involved; the approximate number of affected individuals, if known, and other pertinent data. The attached form should be used for that purpose whenever reasonably possible.

Employees who in good faith report a potential or actual breach under these guidelines will not be subject to retaliation for making such a report.

Subpart B. Breach Affected Division Response Process. After a potential breach of data security has been reported the responsible authority will work with the affected department or office to take necessary steps to contain and control the integrity of the data handling systems impacted by the potential or reported breach and conduct a preliminary internal assessment of the scope of the potential breach. Applicable Information Technology (IT) staff and security procedures or other guidelines may be consulted as set forth in this policy.

If the potential breach is on a county computing system that contains or has network access to private or confidential data, the Responsible Authority shall consult with IT personnel and consider control measures that may include but are not necessarily limited to removing the computing system from the network.

(a) **Determining Breach**. The Responsible Authority shall consult with the affected staff supervisor to determine whether a breach of security of data has occurred.

(b) **Incidents**. Examples of the types of incidents that may result in a notice-triggering breach include, but are not limited to:
   i. Evidence of unauthorized access into a computer system containing private/confidential data;
   ii. Missing documents or papers or stolen or missing laptop, desktop, storage device or other types of information technology resource containing files with private/confidential data;
   iii. Documents containing private/confidential data sent in any form to a wrong recipient;
   iv. IT Systems containing private/confidential data that has been compromised; or
   v. Employee misuse of authorized access to or disclose of private or confidential data.

(c) **Acquisitions**. Minn. Stat. Sect. 13.055, subd. 2 requires government entities to notify individuals if their private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. In making that determination the following factors among others may be considered:

i. Indications the data is in the physical possession and control of an unauthorized person such as a lost or stolen computer or other device or documents containing unprotected private or confidential data.
ii. Indications the data has been downloaded or otherwise acquired.
iii. Indications the data was used by an unauthorized person such as a fraudulent account opened or an instance of identity theft reported;
iv. The encryption protection of the data, if any;
v. Duration of exposure;
vi. The extent to which the compromise of electronic data indicates a directed attack such as a pattern showing the device itself was specifically targeted; or
vii. Indications the attack was intended to seek and collect private or confidential data.

1. **Timing of Notification**. If a breach has been determined in most instances the affected department or office has primary responsibility to notify affected individuals and may be assisted by the Responsible Authority. Notice is to occur without unreasonable delay. Notice maybe delayed due to a) the legitimate needs of a law enforcement agency; or b) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

   Immediate notification may be appropriate in the event of a breach that could have immediate deleterious impact on individuals whose data may have been acquired by an unauthorized person.

2. **Contacting Law Enforcement.** The Responsible Authority or designee(s) shall contact law enforcement agencies if the breach of security is believed to involve illegal activities. Data may be shared with law enforcement consistent with applicable data practice laws. If law enforcement is contacted it should be informed of the County's practice to provide notice to affected individuals. If law enforcement advises such notice would impede an active criminal investigation notice may be delayed. Delayed notice should be sent out as soon as law enforcement advises it would no longer impede the criminal investigation.

3. **Whom to Notify**. The Responsible Authority in consultation with other appropriate county personnel, including but not limited to the affected department or office, shall determine the scope of the notice. Notice of a breach must be provided to any individual whose private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. If specific individuals cannot be identified notice should be sent to groups of individuals likely to have been affected such as all whose data is stored in the database of files involved in the breach. Measures should be taken to prevent notice lists from being over-inclusive. If questions arise regarding the scope of the notice required, the County Attorneys' Office may be contacted for guidance.

Subpart C. Notice.

1. **Content**. The Responsible Authority or designee shall consult with the affected department or office on the wording of a notice. IT personnel may also be consulted where appropriate. Notices shall generally be sent separate from other documents. The notice should use clear and plain language.

   The following should generally be included in the notice:
   (a) A general description of what happened and when to the extent known.
   (b) The nature of the individual's private or confidential data that was involved, but not listing the specific private/confidential data.
   (c) Information about what the county has done to protect the individual's private/confidential data from further disclosure.
   (d) Institution assistance such as website information or telephone number for further information about the incident.
   (e) Information such as websites about what individuals can do to protect themselves against identity theft including contact information for nationwide credit reporting agencies.

2. **Method of Notification**. The Responsible Authority in consultation with the affected division shall determine the appropriate method of notice as follows.
   (a) **Written notice** by first class mail to each affected individual; or
   (b) **Electronic notice** to each affected individual if communication normally occurs in that medium and the procedure is otherwise consistent with the provisions regarding electronic records and signatures contained in 15 U.S.C. 7001.
   (c) **Substitute notice** may be provided if the cost of providing the written notice required to each affected individual would exceed $250,000 or the affected class of individuals to be notified exceeds 500,000 or the county does not have sufficient contact information to notify affected individuals. Substitute notice consists of all the following:
      (i) **E-mail notice** if the county has an e-mail address for the affected individuals;
      (ii) **Conspicuous posting** of the notice on the county website for a minimum of 45 days and
      (iii) **Notification to major media** outlets that reach the general public.

Subpart D. Coordination with Credit Reporting Agencies. Credit reporting agencies assist individuals in responding to a notice of a security breach. Such agencies should be notified in advance of sending notice of security breach incidents that may significantly increase calls to agencies for assistance.

If notice is required to be given to 1,000 or more individuals at one time the county shall notify without unreasonable delay all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis as defined in 15 U.S.C. 1681a, of the timing, distribution and content of the notice to be sent. Such contacts shall include but not be limited to the following:

- Equifax:
  U.S. Consumer Services
  Equifax Information Services, LLC.
  Phone: 1-800-525-6285

- Experian:
  Experian Security Assistance
  P.O. Box 72
  Allen, TX 75013
  1-888-397-3742

- TransUnion:
  Phone: 1-800-680-7289

Subpart E. Documentation. The responsible authority or designee must complete a Breach of Security Incident Response Summary for each reported breach regardless of whether notice is given. The form should be completed beginning at the time of the initial report or as soon thereafter as reasonably practical.

Where appropriate all documentation related to the breach and investigation shall be labeled and maintained as not public pursuant to the applicable data privacy classification including but not limited to, "security data" as defined by Minn. Stat. 13.37, Subd. 1(a). The form shall be retained by the responsible authority in accordance with the applicable records retention policy.

s

Potential Not Public Data Breach Report

Name of Reporting Person(s): _____

Department or Office: _____

Division: _____

Email: _____

Telephone Number: _____

Date of Report: _____

Time of Report: _____

Date and Time of Discovery of Potential Breach: _____

_____

To Extent Known Date and Time of Potential Breach: _____

_____

Type of Data Involved: _____

_____

Method of Breach to Extent Known or Suspected: _____

_____

Number of Affected Persons: _____

_____

Additional Comments: _____

_____

_____

_____

Signature of Reporting Person

This report must be promptly completed and forwarded to the Aitkin County Attorney. It may be emailed to coatty@co.aitkin.mn.us. Please copy the IT Director at Chris.Sutch@co.aitkin.mn.us.

If you have any questions, please contact the Aitkin County Attorney's Office by emailing coatty@co.aitkin.mn.us or by calling 218-927-7347.