MINUTES
SUMMIT COUNTY
BOARD OF COUNTY COUNCIL
WEDNESDAY, JANUARY 9, 2019
SHELDON RICHINS BUILDING
PARK CITY, UTAH

PRESENT:

Roger Armstrong, Council Chair
Kim Carson, Council Member
Glenn Wright, Council Member

Tom Fisher, Manager
Janna Young, Deputy Manager
Dave Thomas, Chief Civil Deputy
Margaret Olson, Attorney
Kellie Robinson, Chief Deputy Clerk

Council Members Robinson and Clyde were excused from the meeting today.

Council Members attend the Rocky Mountain Power Blue Sky Customer check presentation event, to celebrate the completion of solar panel installation at Richins; Lisa Yoder

Closed Session – Property Acquisition

Council Member Carson made a motion to convene in closed session to discuss property acquisition. The motion was seconded by Council Member Wright and passed unanimously, 4 to 0.

The Summit County Council met in closed session from 3:48 p.m. to 5:10 p.m. to discuss property acquisition. Those in attendance were:

Roger Armstrong, Council Chair
Kim Carson, Council Member
Glenn Wright, Council Member
Chris Robinson, Council Member (via phone)

Tom Fisher, Manager
Janna Young, Deputy Manager
Dave Thomas, Chief Civil Deputy
Margaret Olson, Attorney
Annette Singleton, Executive Assistant
Brian Hanton, SBSRSD
Melissa O’Brien, SBSRSD
Carolyn McIntosh (via phone)

Council Member Wright made a motion to dismiss from closed session to discuss property acquisition and convene in open session. Council Member Carson seconded with all voting in favor, 4-0.
Work Session

Pledge of Allegiance

Discussion regarding Summit County’s response to Utah State Auditor’s Office; Michael Howard, Corrie Forsling, and Matt Leavitt

Michael Howard, Auditor, Corrie Forsling, Treasurer, and Matt Leavitt, Finance Officer, discussed the audit performed by the Utah State Auditor and the letter responding to the findings.
December 31, 2018

Mr. John Dougall (by email jdougall@utah.gov and regular U.S. mail)
Office of the State Auditor
Utah State Capitol Complex
East Office Building, Suite E320
Salt Lake City, UT 84114-2310

Dear Mr. Dougall:

This letter is provided in connection with a recent visit to Summit County from your Local Government Manager, Jeremy Walker on December 10, 2018, with the intention of evaluating County internal controls and providing advice and consultation. Representations in this letter are in response to initial feedback from Mr. Walker's visit and not from any draft report of findings and recommendations. We therefore look forward to further communication from the State Auditor's Office (SAO) to improve methods of separation of duties, general internal controls, and fraud risk.

Summit County is committed to providing essential accountability and transparency over all government programs while upholding ethical behavior and the public trust. We take very seriously our role as stewards of taxpayer dollars and strive for excellence in the areas of accountability, transparency, and fraud protection. As an example of the County's efforts, Summit County is one of only four counties in the State of Utah that goes through the arduous process of preparing an annual Comprehensive Annual Financial Report (CAFR) for its citizens.

Summit County's established system of internal controls is based on standards set forth by the U.S. Government Accountability Office (GAO) and their publications, Generally Accepted Government Auditing Standards (GAGAS, or "The Yellow Book"), 2018 revision, and the Standards for Internal Control in the Federal Government ("The Green Book"), 2014 revision. These standards, while not formally adopted by the County, have provided the framework and reference materials to improve accountability and transparency of County finances.

In addition, Summit County frequently evaluates internal practices and procedures against the State Compliance Audit Guide, most recently the 2017 revision, published by the SAO in conjunction with the annual independent audit. Components of the independent audit include meetings with the audit committee and fraud interviews with employees. While not the only opportunity for employees and officials to express concerns about County operations and practices, it is a formal opportunity provided by the independent auditors and the County. Any trepidations are thoroughly and independently investigated and acted upon.

Further, Title 2 U.S. Code of Federal Regulations Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) requires the County to
report compliance with requirements for federally awarded funds. As a recipient of federal awards, Summit County is required to report Form SF-SAC to the Federal Audit Clearinghouse Image Management System. Form SF-SAC also requires the County to report the fraud risk level as determined by its independent auditors. The County has reported as a "low-risk" auditee for the past three years. The County's Single Audit reports can be found here: https://harvester.census.gov/facdissem/.

Summit County has received the SAO's Fraud Risk Assessment Implementation Guide and is currently comparing the specific measures outlined in the Guide with both the GAO's Yellow Book and Green Book, identifying gaps and implementing steps to close those gaps, ensuring the County's internal controls are as robust as possible.

While we appreciate the SAO providing the Assessment Implementation Guide as it contains useful instructions for counties, we do have some concerns about the Guide and the assessment questionnaire within the Guide being used exclusively by the SAO in determining counties risk level for fraud.

For one, Summit County's risk level for fraud is being evaluated by the SAO in a general context of counties within the State of Utah, the majority of whom are a Commissioner form of government, and not against Summit County's specific form of government. For this reason, Summit County cannot be evaluated correctly against the scoring and methodology of the Fraud Risk Assessment questionnaire included in the Guide.

Moreover, the questionnaire awards 5 points to counties where all Board Members have completed the SAO's online training. Yet, no one in Summit County was made aware of this training or expectation that it be completed until the Utah Association of Counties (UAC) annual convention this past November when a member of the SAO presented it on it (the only exception is Council Chair, Kim Carson who received an email from the SAO asking her to complete the training. However, it was not articulated to Mrs. Carson that this was a requirement of all Board Members).

Summit County has made a concerted effort to get all the County Board Members, including elected officials and appointed individuals who oversee the Special Service Districts, to complete the online training by December 31, 2018. This has been a challenge since many of our Board Members live in rural areas of the County and do not have access to computers. In early January 2019, the County will host a group training in the County seat for all those who are not able to complete the training on their own.

We encourage the Office of the State Auditor to look at ways to improve communication and notification about this training and work with counties to make it easier for Board Members to complete it.

Finally, Mr. Walker's visit on December 10th seemed to be under-represented when the appointment was made, resulting in County staff not feeling as prepared to provide all the information requested as we normally would be for an audit review. As such, we appreciate the opportunity to now provide your office additional documentation and explanation of how we currently comply with the measures outlined in the Fraud Risk Assessment Implementation Guide.
The attached materials are provided to support representations made during Mr. Walker’s visit that Summit County is committed to ethical work performance. In addition, the Fraud Risk Assessment questionnaire has been included on the following page. The County has indexed the SAO’s questionnaire with answers and references to the appropriate supporting documentation, which can be found in the attached binder.

We are confident the additional measures we have implemented from the Fraud Risk Assessment Guide combined with our current practices and procedures have accounted for any gaps in our internal controls, making them as robust as possible and reducing our risk of undetected fraud, abuse and noncompliance.

Again, thank you for your review of this information. Please let us know if you have questions or if we may provide additional information. As with your purpose, we want to make sure that Summit County is trustworthy and accountable to our citizens.

We would also appreciate you confirming receipt of this letter and providing a response by email as to your intent in reviewing this material for your draft and final reports. Once again, thank you for your collaboration and interest in working with us on our internal controls.

Sincerely,

Michael Howard
Auditor

Corrie Forsling
Treasurer

Thomas C. Fisher
County Manager

c. Jeremy Walker, Local Government Manager, Office of the State Auditor (jeremywalker@utah.gov)
Kim Carson, Summit County Council Chair (kcarson@summitcounty.org)
Roger Armstrong, Summit County Council Vice-Chair (ramstrong@summitcounty.org)
Christopher F. Robinson, Summit County Council (cfrobinson@summitcounty.org)
Doug Clyde, Summit County Council (dclyde@summitcounty.org)
Glenn Wright, Summit County Council (gwright@summitcounty.org)
Margaret Olson, Summit County Attorney (molson@summitcounty.org)
Kent Jones, Summit County Clerk (kentjones@summitcounty.org)
Rhonda Francis, Summit County Recorder (rfrancis@summitcounty.org)
Steve Martin, Summit County Assessor (smartin@summitcounty.org)
Justin Martinez, Summit County Sheriff (jmartinez@summitcounty.org)
<table>
<thead>
<tr>
<th>Item</th>
<th>Yes</th>
<th>Pts</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the entity have a formal internal audit function?</td>
<td>X</td>
<td>50</td>
<td>Yes. See Binder Tab 1 for details.</td>
</tr>
<tr>
<td>2. Does the entity have a fraud hotline?</td>
<td>X</td>
<td>35</td>
<td>Yes. See Binder Tab 2 for written policy.</td>
</tr>
<tr>
<td>3. Does the entity have a formal audit committee?</td>
<td>X</td>
<td>20</td>
<td>Yes. Summit County’s formal audit committee is currently comprised of Roger Armstrong (Council Member), Chris Robinson (Council Member), and the independent auditor. The members of the audit committee are assigned at the first Council meeting in January each year when the Council committee assignments are formally made. The independent auditor maintains the records and minutes of the audit committee meetings.</td>
</tr>
<tr>
<td>4. Does the entity have a licensed CPA as part of its management team?</td>
<td>X</td>
<td>10</td>
<td>Yes. Chris Robinson, member of the County Council and formal audit committee has a Bachelor’s degree with honors in accounting. He passed the CPA exam but did not pursue the license.</td>
</tr>
<tr>
<td>a. If no, do any members of the management team have a bachelor’s degree in accounting?</td>
<td>X</td>
<td>10</td>
<td>The County’s Financial Officer, Auditor and Treasurer, as members of the management team, hold either a Bachelor’s or Master’s degree in Business Administration.</td>
</tr>
<tr>
<td>5. Regardless of license or formal education, does at least one member of the management team receive at least 40 hours of formal training related to accounting, budgeting, or other financial areas each year?</td>
<td>X</td>
<td>15</td>
<td>Yes. Summit County’s Financial Officer, Auditor and Treasurer, along with staff in the Auditor and Treasurer’s offices attend the annual GFOA conference, annual Utah Association of Counties conference, and county Auditor and Treasurer association conferences, complete online classes, study current financial publications and professional literature related to budgeting, accounting and financial best practices each year.</td>
</tr>
<tr>
<td>6. Are employees and elected officials required to annually commit in writing to abide by a statement of ethical behavior?</td>
<td>X</td>
<td>10</td>
<td>Summit County is in the process of implementing a 45-minute training requirement on ethical behavior utilizing a course provided by the Utah Local Governments Trust, which every employee will be required to complete by the end of April every year. At the end of the training, each employee will sign a form indicating s/he has completed the training and will abide by its contents. This is provided to the Trust who then sends it to Summit County’s Personnel Department.</td>
</tr>
<tr>
<td>7. Have all the board members completed the State Auditor online training at least once in the last four years?</td>
<td>X</td>
<td>2</td>
<td>In Progress. All five County Council members, County Manager, and 10 of 31 Board Members of the County’s Special Service Districts have completed the online training this year. The remaining 21 Board Members of the Special Service Districts are in the process of completing the training by the end of December 2018. The County Council has been diligently working on getting every Board Member in compliance with this measure since first finding out about the online training mid-November 2018. Some of our rural-located Board Members do not have email addresses or access to a computer, which has added to the challenge of everyone completing the training. The Council will host a group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>training session in early January 2019 in the County seat for all remaining Board Members yet to complete the training by December 31, 2018. See Binder Tab 3 for certificates.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>8. Does the entity have written policies in the following areas:</strong></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
<td><strong>a. Reporting fraud and abuse?</strong> Yes. See below.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td><strong>b. Conflict of interest?</strong> See Binder Tab 5, Section 12-2 of the Summit County Personnel Manual</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td><strong>c. Ethical behavior?</strong> See Binder Tab 6, Title 17, Chapter 16 and Title 52, Chapter 3, of Utah State Code deal specifically with the ethical conduct of County officers and employees. The Summit County Personnel Manual, sections 10, 11, 12, 16, 17 and 18, are reviewed regularly to ensure compliance with these state code provisions. Also, Summit County will be implementing annual ethical behavior training offered by the Utah Local Government Trust starting in 2019 in conjunction with other risk reducing annual trainings that all employees complete.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td><strong>d. Travel?</strong> See Binder Tab 7, section 10-1 of the Summit County Personnel Manual</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td><strong>e. Credit/Purchasing cards (where applicable)?</strong> See Binder Tab 8, Summit County Auditor policy and form completed by all purchasing card holders</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td><strong>f. Cash receipting and deposits?</strong> See Binder Tab 9, Summit County Treasurer Policy</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td><strong>g. Procurement?</strong> See Binder Tab 10, Title 1, Chapter 16 of Summit County Code as amended by the Summit County Council on 8/13/15</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td><strong>h. Personal use of entity assets?</strong> See Binder Tab 11, Section 18 of the Summit County Personnel Manual addresses the use of entity assets</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td><strong>i. IT and computer security?</strong> Section 18 of the County's Personnel Policy was revamped a couple of years ago to deal with security involving social media, personal devices, and county owned devices. The County's IT Department went through a CJIS audit with the FBI at the Justice Center in October/November 2018. One thing they noted was we needed to have a written IT Policy. The FBI provided templates, which we have modified for our County. We also sent 70 employees, mostly those dealing with financial transactions, to a 2-hour cybersecurity training program earlier this year. See Binder Tab 12 for copies of the IT and computer security policies.</td>
<td></td>
</tr>
</tbody>
</table>

**Total Points: 170, Very Low Risk Level**

Complted By: [Signature]
Thomas C. Fisher, County Manager
Completion Date: 1/31/18
Tab 1
December 28, 2018

Mr. John Dougall
Utah State Auditor
East Office Building, Suite E310
Utah State Capitol Complex
Salt Lake City, UT 84114

RE: Summit County Internal Control System Monitoring

Dear Mr. Dougall,

This letter is provided in connection with the recent visit of Mr. Jeremy Walker to Summit County on December 10, 2018. Our understanding of the purpose of Mr. Walker's visit was to evaluate County internal controls and to serve as a consultation resource to our leadership team. We appreciate his time and efforts in helping us to improve our controls and processes along with explaining the new "Resource" page from the State Auditor's Office (SAO) website.

We now wish to provide more information regarding Question #1 from the SAO's Fraud Risk Assessment questionnaire: “Does the County have a formal internal audit function?” We interpret this question as “Does the County have an ongoing monitoring function?” Our answer to the question is “yes.” The interpretation of the question and our answer is based on the County’s usage and adherence to generally accepted principles found in both the “Yellow Book” and the “Green Book” published by the U.S. Government Accountability Office (GAO).

**Principle 16.05** of the “Green Book” specifies that “ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations and other routine actions.” **Principle 16.06** states that “The scope and frequency of separate valuations depend primarily on the assessment of risks, effectiveness of ongoing monitoring and rate of change within the entity and its environment.” **Principle 16.07** explains that “Separate evaluations also include audits and other evaluations that may involve the review of control design and direct testing of internal control.”

The County has several ongoing monitoring functions that are performed regularly along with some on an “as-needed” basis. A partial list of examples follows:

1. The Treasurer Trust Account is being reconciled by the County Auditor each month.

2. All payroll disbursements are reviewed and approved by the County Auditor, County Treasurer and the County Manager.
3. All A/P Transactions (including wires, checks and ACH) are reviewed and approved by the County Auditor, County Treasurer and the County Manager. Dual signatures from separate departments are required before payments are released.

4. Vendor ACH financial account changes are reviewed and verified by the County Auditor via phone to the vendor number on file.

5. Yearly monitoring audits are performed on all receivables/payables, payroll trust, petty cash, Federal, State and miscellaneous grants, Internal Restaurant Tax and RAP tax grants, transit fund revenue vs. expense, landfill receipting, amended budgets, Insurance Fund and bank account, waste department revenue and expense, etc.

6. Quarterly monitoring audits are consistently performed on the Corrections trust revenue and expense vs. bank account, Federal Seizure trust revenue and expense, building permit state surcharge vs. Summit County accounts, bail and inmate accounts, all bond trust accounts, ambulance reimbursement, etc.

7. An audit is currently underway at the Planning Department with regards to new online permit software vs financial records.

8. Payroll time card audits are conducted both on a randomized time frame and in response to potential fraud reports.

The above examples are illustrative of the commitment expressed by County Leadership to reducing all aspects of the Fraud Triangle and help ensure that taxpayer funds go to the programs desired by the Citizens of Summit County.

In conclusion, we appreciate this opportunity to further explain our "ongoing monitoring function" in more detail to you. We also want to again thank you, and your staff, for being a valuable resource to the County in addition to our Independent and Dependent Districts as we consistently and progressively pursue the protection of taxpayer funds and trust.

Sincerely,

Michael Howard, MBA
Summit County Auditor
Tab 2
FRAUD REPORTING POLICY

A. Purpose

Summit County is committed to transparency and accountability in the utilization of taxpayer and other funds for County operations. In support of this commitment, the County has established a process that taxpayers, employees and contractors should use to report suspected fraudulent use of these monies.

B. Definitions

Internal Review Committee (IRC): committee consisting of three members, the County Auditor, the County Attorney and the County Manager. The functions of the IRC are outlined in this policy.

Audit Committee (AC): committee consisting of the County's contracted external independent auditor along with two (2) members of the County Council. The duties of the AC relating to fraud reporting closely follow those outlined in this policy.

C. Filing a Complaint

1. Complaints may be submitted to the IRC either via telephone, email, or in writing.
   Email: auditorhotline@summitcounty.org
   Phone: (435) 336-3207
   Writing: Summit County IRC – P.O. Box 128, Coalville, UT 84017

2. Complaints regarding any member of the Internal Review Committee should be reported directly to the Audit Committee. The Audit Committee will then follow the steps in this policy to determine the proper course of action. Submit the complaint to the following individuals: Chris Robinson, Member Summit County Council, at: cfrobinson@summitcounty.org and Roger Armstrong, Vice Chair Summit County Council, at: rarmstrong@summitcounty.org.

D. Information to Report

1. The submitter should, to the extent possible, provide the following relevant pieces of information in their complaint:
   a. The name of the individual who the complaint is made against. The position, department, supervisor and phone number of the individual committing the alleged activity if known.
   b. Contact information of the person making the allegation.
   c. Alleged improper behavior described in detail.
   d. Date(s), time(s) and frequency of the alleged improper activity.
   e. Location where the alleged event(s) occurred.
f. Contact information for corroborating witnesses (if any).

g. Evidence or documentation supporting the allegation.

E. Investigative Process

1. Once the complaint has been received by the Internal Review Committee (IRC), it will undergo a series of steps to determine validity, appropriateness and priority. The IRC will consider the following factors during screening and prioritization:

a. Does the complaint involve actions by an individual subject to Summit County’s authority? *Examples include:* Dependent Special Service Districts, management or employees of Summit County.

b. Do the allegation(s) explicitly pertain to improper governmental activities? *Disagreements over management decisions or actions taken by elected officials, department heads or supervisors that are within the law will not be investigated.*

c. What is the timing and frequency of the alleged improper activity? *Allegations of improper activities that are more recent and/or on-going may receive a higher priority and resource commitment.*

d. Can the complaint be efficiently and effectively investigated? *Overly broad, vague or complaints with minimal to no supplied evidence may be rejected or assigned a low priority.*

2. The IRC determines the disposition of the complaint:
   a. Decline to investigate the complaint; or
   b. Accept the complaint and begin an investigation; or
   c. Refer the complaint to an outside investigative agency.

3. If the IRC decides to pursue an investigation, it will determine:
   a. Timeframe for the audit; and
   b. Budget and resource allocation; and
   c. Scope of the audit.

4. The Auditor/investigative agency conducts the audit and issues a report to the IRC along with any findings and/or recommendations.

5. The IRC presents the report to the County Council.

6. The County Council or their designee addresses any findings noted in the report.

F. Whistleblower Protection

*Utah Code § 67-21-3 prohibits public employers from taking adverse action against their employees for reporting government waste or violations of law in good faith, to the appropriate authorities. A public entity employee, public body employee, legislative*
employee, or judicial employee, is presumed to have communicated in good faith if they have given written notice or otherwise formally communicated the conduct to the entity (see Utah Code § 67-21-3(1)(b)(iv)(A) for more information).

G. **Confidentiality**

The identity of the complainant is considered protected information under the Utah Government Records Access and Management Act (GRAMA) and will be kept confidential if requested by the individual making the allegation. (See Utah Code Section 67-3-1(15)).

Complaints may be submitted anonymously. However, it is preferable that the person making the allegation to provide their name and contact information. This information allows for follow-up questions and reporting the results. Whistleblower protections do not apply to anonymous complaints.
CERTIFICATE OF COMPLETION

Robert Richer

has successfully completed

Board Member Training

Office of the Utah State Auditor

December 28, 2018
CERTIFICATE OF COMPLETION

Tor Boschen

has successfully completed

Board Member Training

Office of the Utah State Auditor
Office of the State Auditor

December 22, 2018
CERTIFICATE OF COMPLETION

Kim Carson

has successfully completed

Board Member Training

October 18, 2018
Certificate: 12297558

CERTIFICATE OF COMPLETION

Charles Dinger

has successfully completed

Board Member Training

December 23, 2018

Office of the Utah State Auditor
Office of the State Auditor
CERTIFICATE OF COMPLETION

Jay Dyal

has successfully completed

Board Member Training

December 26, 2018

Office of the State Auditor

State of Utah
Certificate: 12284368

CERTIFICATE OF COMPLETION

Thomas Fisher

has successfully completed

Introductory Training for County Officials

Office of the Utah State Auditor

December 19, 2018
Gale Pace
Show All Credentials

OPTIONS:
If this is your credential...
Sign in to access disabled or private options

LinkedIn
Download PDF
Email Credential
Embed Credential

Contact Office of the State Auditor
Help

CERTIFICATE OF COMPLETION

Gale Pace
has successfully completed
Board Member Training

STATE OF UTAH
Office of the State Auditor
December 21, 2018

Board Member Training
Office of the State Auditor

ISSUED ON
December 21, 2018

EXPIRES ON
Does not expire

This certificate certifies that the learner has completed Board Member Training.
Further information...

OTHER COURSES FROM THIS ISSUER
CERTIFICATE OF COMPLETION

Catherine Kahlow

has successfully completed

Board Member Training

Office of the State Auditor

December 24, 2018
Certificate: 12302460

CERTIFICATE OF COMPLETION

Mike Kobe

has successfully completed

Board Member Training

Office of the State Auditor

Office of the State Auditor

December 27, 2018
CERTIFICATE OF COMPLETION

Gary Resnick

has successfully completed

Board Member Training

Office of the State Auditor
Office of the State Auditor

December 22, 2018
Certificate: 12181143

CERTIFICATE OF COMPLETE

Ian Schofield

has successfully completed

Board Member Training

Office of the State Auditor

Office of the State Auditor

November 20, 2018
CERTIFICATE OF COMPLETION

Certificate: 12296115

Vern Williams

has successfully completed

Board Member Training

Office of the Utah State Auditor
Office of the State Auditor

December 22, 2018
Glenn Wright
Summit County Council

---

From: noreply@notify.thinkific.com <noreply@notify.thinkific.com> on behalf of Office of the State Auditor - Training Portal <noreply@notify.thinkific.com>
Sent: Wednesday, December 19, 2018 1:54 PM
To: Glenn Wright
Subject: Board Member Training 2018 Completed

Office of the State Auditor - Training Portal

Congratulations Glenn,

You have completed the Board Member Training 2018 course.
Sincerely,
Office of the State Auditor

Login to your account | Edit notification settings
CERTIFICATE OF COMPLETION

Suzanne Carpenter

has successfully completed

Board Member Training

Office of the State Auditor

December 23, 2018
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
FRAUD REPORTING POLICY

A. **Purpose**

Summit County is committed to transparency and accountability in the utilization of taxpayer and other funds for County operations. In support of this commitment, the County has established a process that taxpayers, employees and contractors should use to report suspected fraudulent use of these monies.

B. **Definitions**

*Internal Review Committee (IRC)*: committee consisting of three members, the County Auditor, the County Attorney and the County Manager. The functions of the IRC are outlined in this policy.

*Audit Committee (AC)*: committee consisting of the County's contracted external independent auditor along with two (2) members of the County Council. The duties of the AC relating to fraud reporting closely follow those outlined in this policy.

C. **Filing a Complaint**

1. Complaints may be submitted to the IRC either via telephone, email, or in writing.
   Email: auditorhotline@summitcounty.org  
   Phone: (435) 336-3207  
   Writing: Summit County IRC – P.O. Box 128, Coalville, UT 84017

2. Complaints regarding any member of the *Internal Review Committee* should be reported directly to the Audit Committee. The Audit Committee will then follow the steps in this policy to determine the proper course of action. Submit the complaint to the following individuals: Chris Robinson, Member Summit County Council, at: crobinson@summitcounty.org and Roger Armstrong, Vice Chair Summit County Council, at: rarmstrong@summitcounty.org.

D. **Information to Report.**

1. The submitter should, to the extent possible, provide the following relevant pieces of information in their complaint:
   a. The name of the individual who the complaint is made against. The position, department, supervisor and phone number of the individual committing the alleged activity if known.
   b. Contact information of the person making the allegation.
   c. Alleged improper behavior described in detail.
   d. Date(s), time(s) and frequency of the alleged improper activity.
   e. Location where the alleged event(s) occurred.
f. Contact information for corroborating witnesses (if any).

g. Evidence or documentation supporting the allegation.

E. Investigative Process

1. Once the complaint has been received by the Internal Review Committee (IRC), it will undergo a series of steps to determine validity, appropriateness and priority. The IRC will consider the following factors during screening and prioritization:

   a. Does the complaint involve actions by an individual subject to Summit County’s authority? Examples include: Dependent Special Service Districts, management or employees of Summit County.

   b. Do the allegation(s) explicitly pertain to improper governmental activities? Disagreements over management decisions or actions taken by elected officials, department heads or supervisors that are within the law will not be investigated.

   c. What is the timing and frequency of the alleged improper activity? Allegations of improper activities that are more recent and/or on-going may receive a higher priority and resource commitment.

   d. Can the complaint be efficiently and effectively investigated? Overly broad, vague or complaints with minimal to no supplied evidence may be rejected or assigned a low priority.

2. The IRC determines the disposition of the complaint:
   a. Decline to investigate the complaint; or
   b. Accept the complaint and begin an investigation; or
   c. Refer the complaint to an outside investigative agency.

3. If the IRC decides to pursue an investigation, it will determine:
   a. Timeframe for the audit; and
   b. Budget and resource allocation; and
   c. Scope of the audit.

4. The Auditor/investigative agency conducts the audit and issues a report to the IRC along with any findings and/or recommendations.

5. The IRC presents the report to the County Council.

6. The County Council or their designee addresses any findings noted in the report.

F. Whistleblower Protection

Utah Code § 67-21-3 prohibits public employers from taking adverse action against their employees for reporting government waste or violations of law in good faith, to the appropriate authorities. A public entity employee, public body employee, legislative
employee, or judicial employee, is presumed to have communicated in good faith if they have given written notice or otherwise formally communicated the conduct to the entity (see Utah Code § 67-21-3(1)(b)(iv)(A) for more information).

G. Confidentiality

The identity of the complainant is considered protected information under the Utah Government Records Access and Management Act (GRAMA) and will be kept confidential if requested by the individual making the allegation. (See Utah Code Section 67-3-1(15)).

Complaints may be submitted anonymously. However, it is preferable that the person making the allegation to provide their name and contact information. This information allows for follow-up questions and reporting the results. Whistleblower protections do not apply to anonymous complaints.
5. If the department head determines that either the employment or payment could reasonably present a real or potential conflict of interest, the department head shall deny permission. The department head's decision may be grieved. Failure to notify the employer and to gain approval is grounds for disciplinary action. Employees may jeopardize their employment with the County through unsatisfactory performance reviews affected by outside employment.

C. Conflict Of Interest
Employees shall not use their County position or any influence, power, authority, confidential information derived there from, or County time, equipment, property, or supplies for private gain. Employees shall not receive outside compensation for their performance of County duties except in cases of:

1. Awards for meritorious public contribution publicly awarded.

2. Receipt of honoraria or expenses paid for papers, speeches, or appearances made by employees with the approval of the department head, or on their own time for which they are not compensated by the County, nor prohibited by these rules.

3. Receipt of usual social amenities, ceremonial gifts, or insubstantial advertising gifts as established by state law (See Section 17, Paragraph B). When an employee's responsibilities require an action or a decision which could be interpreted as a conflict of interest, the employee shall declare the potential conflict. The department head may then determine and notify the employee of the status of the potential conflict, either approving of the activity or listing the objections of the County.

Cl. Non-competition
Summit County has an interest in preserving the integrity of information created, received or kept as part of its governmental business and processes. As a result, any employee who is separated from the County shall be prohibited from using information classified as private, controlled or protected, and gained during their employment, in any manner which may be contrary to law or adverse to the County when representing their private interests after separation. Further, in order to protect the integrity of the processes and to ensure equitable treatment to all persons dealing with the County, former employees who, as part of their County duties, worked with or assisted any group, individual or entity in achieving benefits from the County, shall not privately represent or assist those same groups, individuals or entities, in county matters, for a period of at least six (6) months after separation from the County.
Tab 6
Tab 7
SECTION 10 - REIMBURSEMENT FOR EXPENSE

A. **Travel**

   Revised 7-30-2015

   Travel expenses associated with authorized trips on County business, for attendance at conventions, conferences, field trips, seminars, educational courses or meetings etc., will be paid by the County. It is the County’s policy that the most cost effective travel and training shall be pursued to accomplish the training goals of each division and department. Actual costs for materials required for the seminar, training courses, etc., will be paid for or reimbursed by the County.

   If the employee expends personal funds required for travel, for reasonable expenses, the employee will provide receipts/ledger of expenses to the County upon completion of the trip, but not later than one week after return to normal duties. For specific policies regarding meal reimbursement please see paragraph 6 of this section.

   An employee may be accompanied by a spouse or family member on approved County business trips with the understanding that the County will not pay any of the costs incurred by the spouse or be responsible for any liability associated therewith.

   Department Heads shall have approval authority for all travel when travel coincides with the employee’s professional associations and/or training and has been pre-approved by the County Council in the departmental travel budget. All travel and mileage vouchers shall be signed by the Department Head.

   To accomplish the County’s goals the following guidelines and procedures shall be followed for expenditure and reimbursement of travel associated expenses:

   1. Public Transportation or Car Rental: The most economical available means of transportation shall be used, considering travel time, fares, convenience and liability. Receipts will be required in the event reimbursement is necessary.

   2. Miscellaneous Transportation: Toll charges, parking fees, non-receiptable fares for taxi, buses, etc., shall be reimbursed at actual cost. Fuel, emergency repairs, towing charges, storage fees, etc., for County vehicles will be reimbursed with receipts.

   3. If more than one employee from the same division is traveling to the same event and/or location by automobile, carpooling in a county vehicle is strongly recommended. If personal transportation is used only one mileage reimbursement per event/location shall be allowed.

   4. Lodging: Receipts will be required in the event reimbursement is necessary. If an employee travels and stays with friends or relatives rather than in a hotel/motel the employee may be reimbursed at the rate of $40.00 per day without receipts, with prior approval of the Department Head.
5. Personal Transportation: Personal vehicles may be used if County vehicles are not available. For travel out-of-state, county vehicles will not be used, unless authorization is obtained from the County Manager. Reimbursement for personal car use shall be at the rate as published in I.R.S. Publication 463 and adjusted yearly.

   a. When two or more employees travel in a private car, only one employee will be reimbursed for vehicle costs.

   b. Damage to a traveler's personal vehicle occurring during the course of conducting official business is the responsibility of the individual.

   c. Mileage will be computed using either the state mileage charge, or an online mapping program using the most direct route.

   d. Reimbursement will not be allowed for commuting between the traveler's place of residence and the office considered the principal place of assignment or for miles traveled for purposes other than official business.

   e. Computation of mileage should commence from the office considered the principal place of assignment to the point of destination unless the distance from the point of origin other than the principal office to the destination is less.

6. Meals: Meals are allowable on a reimbursable basis for department approved travel outside the County. Use of the per diem rates is the preferred method for meal reimbursement. Meals shall be reimbursed either at actual cost, or at the per diem schedule presented in the most recent edition of the IRS publication 463, whichever is less.

   a. A traveler is entitled to meals when not staying overnight when:

      1) Breakfast - round trip travel is out of County and commences prior to 6:00 a.m.

      2) Lunch - when the trip meets one of the following conditions: The traveler is on an officially approved trip of such duration as to warrant entitlement to breakfast and dinner. The traveler leaves their "home base" before 11:00 a.m. and returns after 2:00 p.m.

      3) Dinner - round trip travel is out of County and arrival back home is later than 7:00 p.m. If meals are complimentary of a hotel, motel, and/or association, no reimbursement will be made for that meal.

Money may be advanced for anticipated expenses.

7. Miscellaneous Expense: Registration fees, incidental supplies, publications, etc., shall
be purchased in advance through the County if possible. Receipts will be required for reimbursement of authorized expenses.
SUMMIT COUNTY COMMERCIAL/PURCHASING CARD POLICY AND ACCEPTANCE

The Summit County Commercial/Purchasing Card issued to you represents the trust Summit County places in you as an employee. You are empowered as a responsible agent to safeguard County assets and to wisely spend taxpayer funds. Your signature below is verification that you have read, understand, accept and agree to comply with this Employee Commercial/Purchasing agreement along with Summit County’s policy on the use of your Commercial/Purchasing card.

Summit County Commercial/Purchasing Card Number: ____________________________

1. I understand that the Card being issued to me is for County approved purchases only, and I agree to not use it for personal expenses. **Don’t place yourself in a difficult situation for when account audits occur.**

2. Improper use of this Card is considered a misappropriation of County Funds which may result in possible disciplinary action up to and including termination of my employment and the taking of legal action against me to recoup the misappropriation.

3. If my card is lost or stolen, I will immediately notify the Summit County Auditor’s office by telephone. I will follow-up the telephone call with an email or facsimile notification to the County Auditor.

4. I agree to surrender the Card to my supervisor immediately upon termination of employment.

5. The Commercial/Purchasing card has been issued in my name. I agree to monitor and approve usage of this card. I accept that I am responsible for any transactions to this card.

6. All purchases are billed directly to Summit County and are paid for with County Funds. In the case of improper use of the card, payments will be made directly to Summit County. I acknowledge and accept that the Card service company cannot accept monies from any other entity other than Summit County. Accordingly, **any personal charges billed to Summit County could be considered a misappropriation of County funds.**

7. I understand and agree to fully comply with current and future internal control procedures and audits.

8. **I agree to photograph and submit electronically all receipts received for purchases made with the Card. If a receipt and/or satisfactory explanation for the purchase(s) is/are not received, the purchase(s) may be considered a misappropriation of County Funds.**

9. Each department head, or duly assigned designee, will reconcile and code transactions monthly to the appropriate County General Ledger funds and accounts. I agree to resolve discrepancies with appropriate parties.

10. I understand that a Commercial/Purchasing Card is not provided to all employees. My assignment of a card is based upon my job functions within the County as well as trustworthiness. I acknowledge that my Card may be revoked at any time and for any reason.

__________________________  ____________________________
Employee Signature / Date          Auditor Signature / Date

__________________________
Employee Printed Name

60 North Main  •  P.O. Box 128  •  Coalville, UT 84017
Phone (435) 336-3016
Tab 9
SUMMIT COUNTY TREASURER
CASH MANAGEMENT POLICY
July 2011

This policy includes The Summit County Treasurer's Procedures for cashiering different types of payments. The term "payment" includes coin, currency, checks, debit and credit cards.

CASH HANDLING
The following are business rules for handling and cashiering a cash payment.
- When accepting cash for a transaction payment, count and state out loud the amount received from the customer.
- To protect the Customer Service Representative (CSR) when making change, the amount received from the customer shall not be placed in the cash drawer prior to making change.
- Change shall be counted twice; first when taking the change out of the drawer and again when it is counted back to the customer.
- Always count out loud the amount of change due to the customer and place the change directly on the counter in front of the customer.
- Place the cash received from the customer in the cash drawer.

CHECK HANDLING
The following is the criteria needed to make a check acceptable:
- Checks shall be written to Summit County or to the Summit County Department and endorsed payable to the order of Summit County or Summit County Treasurer.
- Checks shall be written for the correct amount, do not give change back on checks.
- No two party or counter checks may be accepted.
- Read the amount from the check received.
- All checks shall be validated using the slip printer or endorsement stamp.
- Checks shall be placed in your cash drawer upon completing the transaction.
- All payments will be deposited daily or not more than every three days.
- Construction lien releases must be completed and signed by the department prior to issuing a receipt.
- All checks over $10,000 must be deposited within one business day.

DEBIT CARD PAYMENT HANDLING PROCEDURE
- The customer will swipe their debit card through the card reader and enter their Personal Identification Number (PIN).
*If the transaction is accepted, the customer’s receipt will print on the laser printer after the transaction is finalized.
*If the debit card cannot be read, with the customer’s approval the debit card may be ran as a credit card and hand entered. Debit card information cannot be hand entered.
*Do not give cash back on debit card payment.

CREDIT CARD PAYMENT HANDLING BUSINESS RULES
The following are the business rules for processing a credit card payment.
*When cashiering a credit card payment the customer will swipe the credit card through the card reader.
*If the transaction is accepted the customer will sign the two part receipt that prints on your slip printer.
*The CSR will compare the signature on the card with the signature on the receipt
If the card is not signed the CSR will request a picture identification from the customer.
*The CSR will keep the white copy and place it in their cash drawer with the checks.
*The CSR will give the yellow copy to the customer.
*If the card reader does not read the credit card information, the CSR will hand enter the information.
*If the credit card payment is not accepted the customer can pay with a different payment type

Note: If a credit card cannot be swiped, the CSR can manually enter all required information in the Credit Card Input window, which will appear when the credit card payment type is selected.

Note: The owner of a credit card may not authorize another individual to use his/her card for payment. No exceptions!!

PREVENTING FRAUD
The authorization of a credit card only indicates the availability of the customer’s credit at the time of the transaction, it does not warrant that the person presenting the card is the rightful card member. CSR’s can help to prevent credit card fraud by examining the card presented.

Ways to prevent credit card fraud:
*Watch customer sign receipt.
*Look for signs of tampering on the signature strip of the credit card.
*Compare the signature on the credit card receipt to the signature on the credit card.
*If credit card is not signed or has “see ID” written on the signature line, ask the customer for a form of picture ID.
*CSRs should compare the name on the picture ID to the name on the credit card.
*CSRs should compare the signature on the picture ID with the signature on the credit card receipt.
*CSRs should compare the picture ID to the Customer.
*If the credit card receives authorization but the CSR suspects fraud, they should finalize the transaction and after the customer has left the building they should contact their Manager.

Under no circumstance should a CSR confront a customer about suspected Credit Card fraud.

OFFICE SECURITY – ROBBERY
The purpose of this procedure is to define and describe the County procedures for preventing or responding to a robbery in order to avoid confusion and to assign responsibility for the performance of necessary tasks.

The most important thing to remember in the event of a robbery is to never jeopardize your safety or the safety of others by trying to protect money or other assets.

STAFF PROCEDURE
In the event of a robbery, all employees should take extraordinary measures to ensure their own safety and the safety of other persons who may become involved.

The following guidelines are meant to assist and provide direction to an employee during a robbery.
*Remain calm, cool and observant
*Offer no resistance and comply with the suspect's demands. The money is not worth risking injury or a life. Take no action that could jeopardize the safety of employees or customers.
*Obey the suspect's orders exactly, repeating the order back to the suspect before acting.
*Keep hands in plain view and avoid rapid movements or movements that may be misinterpreted. Explain movements that must be made and why the movement is being made.
*If the suspect displays or claims to have a weapon, assume they do have it and that they would use it.
*If handed a note, pick it up by the corner, place it out of sight and retain if for evidence.
*Make as many mental notes as possible about the suspect, such as, mannerisms, age, height, weight or distinguishing marks (tattoos, scars or birthmarks).
*Note the type of clothing, type of weapon, if jewelry was worn and which hand the weapon was held in.
*Do not block the suspect's escape route.
*Look for a getaway vehicle. Note the color, make, license number, or any distinguishing features (i.e. body damage, as well as the suspect's direction of travel.)
*Note the number of accomplices and their descriptions.
*Activate the Panic button only when it is safe to do so. If the office does not utilize Panic buttons, call police when it is safe to do so.

MANAGEMENT PROCEDURE
Managers must ensure that their employees are prepared in the event of a robbery. To accomplish this, managers should:
*Conduct robbery training at staff meetings.
*Establish assignments for each employee if a robbery occurs. Decide now which employee will lock the doors after the suspect has left the building, who will call the police, who will care for the injured, who will protect the evidence, etc. Do not assume these jobs will be done automatically.

In the event of a robbery, managers should follow these guidelines;
*Dial 911. Make this call even if the panic button has already been activated. Advise them of the robbery and whether injuries have occurred. Give them any information that may be helpful; such as vehicles or suspect descriptions and the direction the suspect took as they left. Remain on the line until officers arrive.
*Verify that everyone (employees and customers) is safe.
*Care for the injured and determine what medical assistance is needed. If medical assistance is needed and was not requested during the 911 call, make an additional 911 call requesting the medical assistance.
*Lock the exterior doors to prevent the suspect from reentering the building.
*Assign someone to wait by the doors to let the law enforcement in when they arrive.
*If applicable, instruct the victimized CSR to lock his or her cash drawer and hand over the keys. The cash drawer should be counted by two people to determine the loss. This should take place after inspection by law enforcement.
*Notify management.
*Keep the office closed until Management provides clearance to reopen.
*Cooperate fully with law enforcement.
*Do not speak with any media and refer all questions to Management.

PUBLIC INTERACTION
During the robbery employees should:
*Try to keep the customers and other employees calm.
*Avoid any action that might increase the potential for harm to you or others.
*Try to prevent customers from taking any action that might increase the potential for harm.
After the suspect has left the building:
* Make sure that everyone (other employees and customers) is safe.
* Do not touch anything that the suspect touched.
* Keep everyone away from the area that the suspect(s) was in
* Do not discuss the robbery among employees or customers until after the police have had the opportunity to interview all those involved.
* Ask all customer witnesses who are present during the robbery or may have witnessed the suspect(s) escape to remain until law enforcement arrives. If customers cannot stay, politely ask for their names, address, and telephone numbers.
Tab 10
Chapter 16
PROCUREMENT OF SUPPLIES, EQUIPMENT AND SERVICES

1-16-1: STATUTORY AUTHORITY:

1-16-2: PURPOSE OF PROVISIONS:

1-16-3: DEFINITIONS:

1-16-4: PURCHASING AGENT:

1-16-5: DEPARTMENT HEADS TO DETERMINE ITEMS TO BE PURCHASED:

1-16-6: PURCHASE CATEGORIES AND AUTHORIZATION:

1-16-7: INVITATION FOR BIDS PROCEDURES:

1-16-8: CONSTRUCTION CONTRACTING MANAGEMENT:

1-16-9: USE OF REQUEST FOR PROPOSALS IN LIEU OF INVITATION FOR BIDS:

1-16-10: RULES AND GUIDELINES FOR REQUEST FOR PROPOSALS:

1-16-11: EXEMPTIONS:

1-16-12: VALUE AMOUNTS:

1-16-13: CHANGE ORDERS:

1-16-14: EMERGENCY PURCHASES:

1-16-15: SUBDIVISION OF PURCHASE PROHIBITED:

1-16-16: INTERLOCAL COOPERATION:

1-16-17: COMPUTER HARDWARE AND SOFTWARE PURCHASES: ADDITIONAL REQUIREMENTS:

1-16-18: PROHIBITED PRACTICES:

1-16-19: DOCUMENTATION AND RETENTION OF BIDS:

1-16-20: PROTESTS:

1-16-1: STATUTORY AUTHORITY


1-16-2: PURPOSE OF PROVISIONS

The purpose of this chapter is to provide for the procuring of supplies, equipment or services by departments and agencies of Summit County in a manner that promotes the best interests of the public; establish the duties, obligations and operational procedures of the County Purchasing Agent and his/her assistants; including appointment procedures and the rules relating to procurement and other related functions.

1-16-3: DEFINITIONS

DEPARTMENT HEAD: The head of any County department or elected official.
INVITATION FOR BIDS: A process of soliciting sealed written bids for goods or services after ten (10) days' notice posted in the County courthouse located at the County seat and publicly distributed through one of the following methods: use of internet purchasing websites, the County website and/or published in a newspaper of general circulation in the County. Invitation for Bids shall be opened by the Purchasing Agent at the time and place stated in the public notice.

LOCAL VENDOR:

A. A business having:

1. A commercial office, store, distribution center, or other place of business located within the boundaries of the County, with an intent to remain on a permanent basis;

2. A current business license in the County or a municipality located in the County; and

3. At least one employee physically present at the local business outlet having published hours of business.

B. The principal place of business of a local vendor may be elsewhere as long as a local branch meeting the above criteria is present. The domicile of one or more partners, owners, associates, directors, employees or agents shall not qualify as constituting a local vendor in the absence of a physical local business outlet within the County.

OFFICIAL: Any Summit County department head, agency head, or elected official making purchases on behalf of Summit County.

OPEN MARKET: Purchasing goods or services on the open market from private vendors.

PURCHASE: The acquisition, by contract or otherwise, of goods or services, by an official on behalf of Summit County.

PURCHASE REQUISITION: A request by a department head (or his/her authorized agent) to the Purchasing Agent to purchase for the requesting department supplies, equipment or services.

PURCHASE ORDER: A County generated document that authorizes a purchase transaction. A purchase order sets forth the descriptions, quantities, prices, discounts, payment terms, date of performance or shipment, other associated terms and conditions, and identifies a specific seller.

PURCHASING AGENCY: Any County department, other than the purchasing office, that is authorized by this chapter or its implementing regulations, or by way of delegation from the Purchasing Agent, to enter into contracts.

PURCHASING AGENT: The individual duly appointed and qualified to act under the direction of the County Manager to negotiate the purchase of or contract for supplies, equipment or services required by the County.
PURCHASING CARD: A credit or debit card issued by a credit card company, bank, or other financial institution and provided by the County to County employees for the purpose of making purchases on behalf of departments of the County.

REQUESTS FOR PROPOSALS: A process of soliciting goods or services through Requests for Proposals delivered to known responsible suppliers and publicly posted in the County courthouse at the County seat.

1-16-4: PURCHASING AGENT

A. Appointment: Pursuant to Utah Code Annotated, section 17-53-307, as amended, and the Summit County Code, section 1-14-10(c)(9), the County Manager shall appoint with the advice and consent of the County Council, a County Purchasing Agent (hereinafter "Purchasing Agent"). The Purchasing Agent shall act under the direction and supervision of the County Manager, to review, coordinate, recommend, and authorize all County purchases or encumbrances as set forth in this chapter.

B. Powers: The Purchasing Agent shall have the following powers:

1. Work cooperatively with and assist Summit County departments, offices and agencies to comply with the purchasing, and procurement regulations as may be established by the County Council and County Manager.

2. Review and approve, pursuant to the requirements outlined in section 1-16-6 of this chapter, purchase requisitions and contracts for the acquisition of supplies, equipment or services for purchases in excess of five thousand dollars ($5,000.00).

3. Assure compliance with bidding and purchasing procedures provided in this chapter.

4. Provide for the transfer of surplus or unused supplies and equipment between departments wherever it can be done effectively.

5. Maintain adequate bidders' lists, vendors' catalog files, and such other records as may be necessary for efficient purchasing activities.

7. Recommend to the Summit County Council, under the direction of the County Manager, for adoption of such rules and regulations as may be reasonable and necessary to clarify and implement the provisions hereof, including additional procedures that may be desirable.

8. Prescribe and update from time to time such forms as may be reasonably necessary for the implementation of this chapter, including, but not limited to, requisitions, purchase orders and bid forms.

9. Revise requisitions or estimates of a department's requirements of supplies and contractual services as to quantity, quality or estimated cost, whenever revision is approved by the department head and deemed to be in the best interests of the County.
C. Delegation Of Authority: The Purchasing Agent may delegate in writing such authority as deemed appropriate to any employees of the office of the Purchasing Agent or of a purchasing agency, respectively, upon approval of the County Manager. Such delegation shall remain in effect unless modified or until revoked in writing.

1-16-5: DEPARTMENT HEADS TO DETERMINE ITEMS TO BE PURCHASED

A. All department heads shall determine what items shall be purchased for their respective departments. Once a determination has been made regarding the items to be purchased, and if the items to be purchased are expected to exceed five thousand dollars ($5,000.00), the department head shall inform the Purchasing Agent of the items to be purchased by submitting a purchase requisition. The Purchasing Agent will work cooperatively with the department head to locate such items at the best available value.

1-16-6: PURCHASING CATEGORIES AND AUTHORIZATION

A. Purchasing Categories: The County classifies purchasing categories. These categories are based on the dollar amount and type of purchases. Each category establishes a separate purchasing limit, authorization level, and procedure.

<table>
<thead>
<tr>
<th>Category</th>
<th>Limitation</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small Purchases</td>
<td>$5,000 or less</td>
<td>Department Head</td>
</tr>
<tr>
<td>Intermediate Purchases</td>
<td>$5,000 to $50,000</td>
<td>Purchasing Agent</td>
</tr>
<tr>
<td>Major Purchases</td>
<td>$50,000 to $500,000</td>
<td>County Manager</td>
</tr>
<tr>
<td>Capital and Special Purchases</td>
<td>$500,000 or more</td>
<td>County Council</td>
</tr>
<tr>
<td>Professional Services</td>
<td>$5,000 or more</td>
<td>County Manager</td>
</tr>
<tr>
<td>Change Orders</td>
<td>$20,000 or more</td>
<td>County Manager</td>
</tr>
</tbody>
</table>

B. Purchasing Authorization:

1. **Small Purchases** - Purchases of supplies, equipment or services less than five thousand dollars ($5,000.00) may be made by the department head (or his/her authorized agent) on the open market. The department head (or his/her authorized agent) is responsible to check for competitive pricing for all purchases and shall retain documentation of pricing and/or proposals for each transaction for a period of thirty six (36) months.

2. **Intermediate Purchases** - In cooperation with the department head, the Purchasing Agent shall make purchases of supplies, equipment or services between five thousand dollars ($5,000.00) and up to fifty thousand dollars ($50,000.00). At the option of the Purchasing Agent, purchases may be made following one of the following three (3) alternatives:

   1. Request for Quote; or
2. Invitation for Bids; or
3. Request for Proposals.

Such bids shall be obtained in writing prior to the acquisition of the requested supplies, equipment or services.

3. **Major Purchases** - In cooperation with the department head, the Purchasing Agent shall prepare, review, and present recommendations to the County Manager for purchases of supplies, equipment or services in the amount of between fifty thousand dollars ($50,000.00) and up to five hundred thousand dollars ($500,000). At the option of the County Manager, purchases may be made following one of the following alternatives:
   a. Invitation for Bids; or
   b. Request for Proposals.

4. **Capital and Special Purchases** – In cooperation with department head, the County Manager shall prepare, review, and present recommendations to the County Council for purchases exceeding the amount of five hundred thousand dollars ($500,000). At the option of the County Manager, with the consultation of the Council, purchases may be made following one of the following alternatives:
   a. Invitation for Bids; or
   b. Request for Proposals.

C. **Purchase Order Required**: Purchase orders shall accompany all purchases with the exception of those made by use of a County issued purchasing card.

**1-16-7: INVITATION FOR BIDS PROCEDURES**

A. Where Invitation for Bids is required, the lowest responsive and responsible bidder shall be determined as follows:

1. **Bid Opening**: Sealed bids shall be submitted as designated in the notice with the statement "Bid for (Item)" on the envelope. Bids shall be opened in public at the time and place stated in the notice. A tabulation of all bids received shall be open for public inspection during regular business hours.

2. **Rejection Of Bids**: The County shall have the authority to reject any or all bids, parts of all bids, or all bids for any one or more supplies or contractual services included in the proposed bid for any reason allowed by law, including, but not limited to, situations where the low responsive and responsible bid exceeds available funds as certified by the appropriate County officer, or when the public interest will be served thereby. Where a bid exceeds available funds and time
or economic considerations preclude resolicitation of work or purchase of a reduced scope or quantity, the County may, at its sole discretion, negotiate an adjustment of the bid price, including changes in the bid requirements, with the low responsible bidder, in order to bring the low bid within the amount of available funds.

3. Tie Bids: If two (2) or more bids received are for the same total amount from equally responsive and responsible bidders, the County may, at its sole discretion, negotiate with the tie bidders, award the bid by lot, or readvertise the bid.

4. Local Preference: If a low bid is submitted by a nonlocal vendor, the bid may be awarded to a responsive and responsible local vendor if the local vendor's bid is within five percent (5%) of the low nonlocal vendor's bid, and if the local vendor agrees, in writing, within seventy-two (72) hours after notification, to meet the low bid. Such notice shall contain the exact bid submitted by the nonlocal bidder, and the County shall not enter into a contract until seventy-two (72) hours have elapsed after notification to the local vendor.

5. Lowest Responsive and Responsible Bidder: In determining who is the lowest responsive and responsible bidder, in addition to price, the County may consider factors relevant to the successful operation of the County's business and the best interests of the County as a whole.

1-16-8: CONSTRUCTION CONTRACTING MANAGEMENT

A. Construction Manager/General Contractor Selection: Pursuant to Utah Code Annotated, section 11-39-107, Summit County may use as one method of construction contracting management a construction manager/general contractor ("CMGC"), as defined in Utah Code Annotated, section 63G-6a-103. If Summit County elects to authorize the use of a CMGC, said CMGC may be selected through a sealed Invitation for Bids procedure, or sealed Request for Proposals in lieu of bids. If sealed proposals are used in lieu of bids, proposals shall be solicited through a Request for Proposals, which shall state the relative importance of price and other evaluating factors. Public notice of the Request for Proposals, describing the position sought and the criteria for the position, shall be given a reasonable time before the date for the opening of the bids. As provided in the Request for Proposals, discussions may be conducted with responsible offerors who submit proposals for the purpose of assuring full understanding of, and responsiveness to, solicitation requirements.

B. Subcontracts While Using A CMGC: When entering into any subcontract that was not specifically included in the CMGC's cost proposal, the CMGC shall procure the subcontractor by using sealed Invitation for Bids or sealed Request for Proposals.

C. Prequalification: Bidders for the position of CMGC may be required to "prequalify" by presenting their state contractor's license, performance bond and other qualifications (e.g., length of time in the business, list of jobs previously done, and written permission to contact previous employers, etc.) at the time they submit their bids.
D. Design Build Provider: A design build provider, as defined in Utah Code Annotated, section 63G-6a-103, may be used as one method of construction contracting management for a Summit County building construction project.

1-16-9: USE OF REQUEST FOR PROPOSALS IN LIEU OF INVITATION FOR BIDS

A. When the Purchasing Agent determines in writing that the use of Invitation for Bids is either not practicable or not advantageous to Summit County, a contract may be entered into by use of a Request for Proposals. Request for Proposals may be used for the procurement of services of consultants or professionals, whether or not the determination described in this section has been made.

1-16-10: RULES AND GUIDELINES FOR REQUEST FOR PROPOSALS

A. Public notice of the Request for Proposals shall be publicly advertised through one of the following methods: use of internet purchasing websites, the County website and/or a newspaper published or of general circulation in the County at least ten (10) days before opening the proposals and shall state the date that proposals shall be submitted. This notice requirement shall not apply in instances of emergency repairs.

B. Proposals shall be opened in public, but the contents of the proposals shall not be disclosed to competing offerors during the process of negotiation except in the case of a local vendor preference under 1-16-7(A)(4). The County may disclose to the public the names of those who have submitted proposals to the County.

C. A register of proposals shall be prepared and filed in the office of the Summit County Purchasing Agent, which shall be open for public inspection after the contract is awarded.

D. The Request for Proposals shall state the relative importance of price and other evaluating factors, and shall state the period of time in which the submitted proposal must remain valid.

E. Discussions may be conducted with responsible offerors who submit proposals for the purpose of assuring full understanding of, and responsiveness to, solicitation requirements.

F. In conducting discussions, there shall be no disclosure of any information derived from proposals submitted by competing offerors.

G. Offerors shall be accorded fair and equal treatment with respect to any opportunity for discussion and revision of proposals.

H. Revisions may be permitted after submissions and before the contract is awarded for the purpose of clarifying the offeror's proposal, or obtaining the best and final offers.
I. The contract shall be awarded to the responsible offeror whose proposal is determined in writing to be the most advantageous to the County, taking into consideration price and the evaluation factors set forth in the Request for Proposals. No other factors or criteria shall be used in the evaluation.

J. The contract file shall contain the basis on which the award is made.

1-16-11: EXEMPTIONS

A. To the extent set forth herein or as otherwise required by law, the following purchases are exempt from the requirements of section 1-16-6 of this chapter:

1. Contracts for the repair, alteration or construction of building improvements and public works projects, which must conform to the requirements of Utah Code Annotated section 11-39-101 et seq., as amended.

2. Contracts for the management, maintenance, operation or construction of jails, which must conform to the requirements of Utah Code Annotated section 17-53-311, as amended.

3. Existing contracts for goods or services negotiated prior to enactment of this chapter.

4. Contracts which by their nature are not suited to award on a competitive basis.

5. Purchases that a County official determines can be made at below market cost at a public auction, closeout sale, bankruptcy sale or other similar sale.

6. Exchanges with other public agencies that a County official determines can be made at a savings to the taxpayer.

7. Purchases from vendors on the state of Utah purchasing office bid list or in the NAACO purchasing program.

8. Purchases of supplies, equipment or services produced by Utah correctional industries.

9. Purchases of goods or services approved by the County Manager as necessary to meet an emergency need.

10. Joint purchase agreements with other public agencies and organizations when the County Manager determines the joint purchase agreement to be in the best interest of the County.

11. Professional service contracts for External Auditor as administered through the County Auditor office.

1-16-12: VALUE AMOUNTS
A. Value amounts used herein refer to both unit cost and combined multiple unit cost and a
determination of the estimated value of supplies, equipment or services that have been requested
by purchase requisition shall be made by the Purchasing Agent in determining the applicability of
the bidding procedure after review of the pertinent purchase requisition and specifications.

1-16-13: CHANGE ORDERS

A. A change order form must document any change order for an approved contract. Change orders
shall require the following authorizations:

1. When a change of condition or additional work is required to continue the orderly progression
of an authorized project, a change order shall be prepared by the department head directing the
work to be accomplished at contract unit prices, an agreed upon lump sum price or as provided
for by contract.

2. Change orders, either singly or in aggregate, or in aggregate with adjustments in individual bid
items, for less than twenty thousand dollars ($20,000) or up to ten percent (10%) of the contract
price, whichever is greater, and within the appropriated budget, may be authorized by the
department head and the Purchasing Agent.

3. Change orders, either singly, or in aggregate, or in aggregate with adjustments in individual bid
items, in excess of the limits placed in 1-16-13(A)(2), must be preauthorized by the County
Manager. However, such change orders may be approved by the department head and the
Purchasing Agent and submitted to the County Manager for ratification under the following
circumstances:

a. The failure to immediately issue a change order may result in significant project cost
   increases or an unacceptable project delay due to work stoppage or other inefficiencies; and

b. Funding for the change order is currently available within the appropriated budget.
   Additional contract work outside the scope of work as defined in the contract or in excess of
   the appropriated budget requires approval by the County council and a supplemental
   appropriation.

4. Notwithstanding the above change order authorizations, the department head and Purchasing
Agent may authorize emergency changes in work outside the original scope of work or in excess
of the appropriated contract. For the purpose of this subsection, an emergency condition will
exist if the failure to act immediately will endanger the public health, safety or welfare or will
jeopardize the fiscal position of Summit County. Such emergency action shall be reported in full
to the County Manager within seventy two (72) hours.

1-16-14: EMERGENCY PURCHASES
A. In certain situations, such as, but not limited to, during the declaration of an emergency, it may be necessary to make emergency purchases, which shortcut the preapprovals required for intermediate or major purchases, as outlined in this chapter. An emergency purchase may be made when there is an immediate need to acquire a particular good or service not already available to County staff. For purposes of this section, an emergency situation is one in which there is an immediate threat to life or property or in which there is or would be a complete disruption of a vital public service. The emergency must be of such a nature and severity that the department head would be immediately notified, regardless of time of day.

B. An emergency purchase of up to twenty thousand dollars ($20,000.00) or less must be preapproved verbally by the appropriate department head. An emergency purchase over twenty thousand dollars ($20,000.00) must be preapproved verbally by the department head and either the County Manager or Purchasing Agent. After an emergency purchase has been made, a purchase order shall be requested from and prepared by the auditor’s office on the next working day. Documentation signed by the department head should include a description of the emergency.

C. In all cases, the County Manager shall be notified within seventy two (72) hours of any and all emergency purchases.

1-16-15: SUBDIVISION OF PURCHASE PROHIBITED

A. No contract or purchase shall be subdivided so as to avoid the requirements of this chapter.

1-16-16: INTERLOCAL COOPERATION

A. Wherever the public benefit can be maximized and costs minimized by entering into joint agreements with other public agencies or organizations for the purchase or construction of any commodity, service or public work, the County shall have the power to so agree, upon approval and action by the County Manager.

1-16-17: COMPUTER HARDWARE AND SOFTWARE PURCHASES: ADDITIONAL REQUIREMENTS

A. To insure compatibility with the County’s existing computer and communication systems, all hardware and software purchases will be reviewed and pre-approved by the director of information technology.

1-16-18: PROHIBITED PRACTICES

A. It shall be unlawful for any officer, agent or employee of the County, or any outside party or entity dealing or seeking to deal with the County to engage in any of the following practices:
1. Collusion or other agreement among bidders or prospective bidders, in restraint of freedom of competition, to fix or in any way rig prices or bids. In addition, any bid tainted with such collusion shall be voidable at the option of the County.

2. Disclosure in advance of the opening of bids of the amount or content of one bid to another bidder or potential bidder. If the County Manager deems such disclosure sufficiently material, he shall void the bidding process and require a new advertisement or invitation for bids.

3. Tender or acceptance of any gratuity in the form of cash, merchandise or other thing of value by a bidder, vendor or contractor to an officer, agent or employee of the County, whether before or after a bid opening or the execution of a contract, which could reasonably be expected to influence him/her in the performance of his/her duties or was intended as a reward for any official action on his/her part.

4. Purchase of supplies or equipment for the personal use of an officer, agent or employee of the County in the name of the County, whether part of a County purchase or contract or separate, and whether paid for with County funds or personal funds of the purchaser. Sole exception shall be where the item or items purchased are required parts of a worker's equipment or uniform and necessary to the successful performance of his duties as a County officer or employee, although personally owned by him.

1-16-19: DOCUMENTATION AND RETENTION OF BIDS:

A. Whenever the County is required by this chapter to receive bids for purchases, construction, repairs, or any other purchase requiring the expenditure of funds, the County department who is in receipt of the bids shall keep all bids received, together with proof of advertisement by publication or otherwise, for at least three (3) years following the letting of any contract pursuant to those bids or three (3) years following the first advertisement for the bids, if all bids pursuant to that advertisement are rejected. Utah Code Annotated section 17-53-225(2).

1-16-20: PROTESTS

A. A person who is an actual or prospective bidder, offeror, or contractor that is aggrieved in connection with a procurement or award of a contract may protest to the County Manager as follows:

1. File a written protest with the County Manager setting forth the protestor's name, physical mailing address, e-mail address, and a concise statement of the grounds upon which the protest is made.

2. The written protest must be received by the County Manager before the opening of bids or the closing date for proposals. However, if the person did not know and should not have known of the facts giving rise to the protest before the bid opening or the closing date for proposals, then
the person must file the written protest within seven (7) calendar days after the day on which the person knows or should have known of the facts giving rise to the protest.

3. A person who fails to timely file a written protest under this section may not bring a protest, action, or appeal challenging a solicitation or award of a contract before the County Manager, the council, a court, or any other forum.

4. The County Manager may enter into a settlement agreement to resolve a protest.

B. After a timely written protest is filed in accordance with 1-16-20(A), the County Manager shall consider the protest and may hold a hearing on the protest.

1. The County Manager may subpoena witnesses and compel their attendance at a protest hearing.

2. The County Manager may subpoena documents for production at a protest hearing.

3. The rules of evidence do not apply to a protest hearing.

4. The County Manager may allow intervention of other parties into a protest.

5. If a hearing on a protest is held, the County Manager shall record the hearing and preserve all evidence presented at the hearing.

6. Regardless of whether a hearing on a protest is held, the County Manager shall preserve all records and other evidence relied upon in reaching the written decision described in 1-16-20(B)(8).

7. The records described in 1-16-20(B)(5) and (6) may not be destroyed until the written decision, and any appeal of the written decision, becomes final.

8. The County Manager shall promptly issue a written decision regarding any protest or contract controversy if it is not settled by mutual agreement. The written decision shall state the reasons for the action taken and inform the protestor, contractor, or prospective contractor of the right to appeal to the Council. The County Manager shall mail, e-mail or otherwise immediately furnish a copy of the written decision to the protestor, contractor, or prospective contractor.

9. If the County Manager does not issue the written decision regarding a protest within thirty (30) calendar days after the day on which a written request for a final decision is filed with the County Manager by the protestor, or within a longer period as may be agreed upon by the parties, the protestor, contractor or prospective contractor may proceed as if an adverse decision had been received.

10. A decision described in 1-16-20(B)(8) is effective until stayed or reversed on appeal.

11. The County Manager may dismiss a protest which is not filed in accordance with the requirements of this chapter.
C. A written appeal setting forth the grounds for the appeal must be filed with the Council within ten (10) calendar days of the date of the written decision of the County Manager.

1. The Council shall presume that the written decision of the County Manager is valid and determine only whether or not the decision is arbitrary or capricious.

2. The Council's review is limited to the County Manager's administrative record. The council may not accept or consider any evidence outside of the County Manager's administrative record.

3. The Council shall issue a written decision regarding any appeal.

   a. The written decision shall state the reasons for the action taken and inform the protestor, contractor or prospective contractor of the right to appeal this final decision of the County to district court within thirty (30) calendar days of the date of the written decision.

   b. The district court's review is limited to the Council's appellate record in the determination of whether or not the Council's written decision is arbitrary or capricious.
Tab 11
SECTION 18 – COMMUNICATIONS

A. Introduction

1. Summit County is committed to implementing new technologies for communication and information exchange, when such will make the County’s employees more productive and increase the County’s capacity to better serve the residents of Summit County. Electronic communication access is provided by the County and is considered County property, its purpose is to facilitate County business, and usage is subject to County control. This policy applies to all electronic communication devices and services which are accessed on or from County premises, are accessed from remote locations using County computer equipment or via County paid access methods. Electronic communication usage includes but is not limited to, telephones, cell phones, pagers, the Internet, social media, radio transmissions, fax transmissions, or email.

2. Communication plays an essential role in the conduct of county business. How employees communicate with the public and with co-workers not only reflects on them individually but also on the County as an organization. The County has invested substantially in information technology and communications systems which enable employees to work more efficiently and employees are expected to use them responsibly and in a manner consistent with these policies.

   a. Electronic communications shall not be used for knowingly transmitting, receiving, retrieving, or storing any communications which are derogatory to any individual or group, are pornographic, lewd, indecent, of a sexual nature, or are of a defamatory or threatening nature. Electronic communications shall not be used in a manner which could be construed as discriminatory based on race, color, religious creed national origin, sex, age, military status, disability, sexual orientation, or gender identification. Electronic communications shall not be used for communication of chain letters, or for any purpose which is illegal, against County policy, or contrary to the County's lawful interests.

3. Although the detailed discussion is generally directed to use of email and internet facilities, the general principles underlying all parts of this policy also apply to telephone communications, fax machines, copiers and scanners.

B. General Principles

1. Employees must use Summit County's information technology and communications equipment sensibly, professionally, lawfully, and consistently with their assigned duties. Employees must show respect for colleagues and for the public and in accordance with these policies and other departmental rules and procedures.

2. With the exception of GRAMA classified protected and private records all information relating to county operations is generally public and must be maintained as such.
3. Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

4. Particular care must be taken when using county email, social media, blogs or internal message boards as a means of communication because all expressions of fact, intention and opinion in an email may bind the employee, and/or the County and can be produced in court in the same way as other kinds of written statements.

5. The advantage of the internet and email is they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. All messages sent on email systems or via the internet should demonstrate the same professionalism as that which would be taken when writing a letter. Employees must not use these media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (as defined by these policies), defamatory, or other unlawful material. If an employee has any question about the appropriateness of any content, they should contact their supervisor for approval.

6. Any messages or information sent via electronic communication, including bulletin board and online services, are statements identifiable and attributable to the County. Use of personal disclaimers with electronic communications will not relieve any user under this policy and users shall be held responsible for any communication initiated by them. All communications sent via a network must comply with this and other County policies and shall not disclose any confidential or proprietary County information.

7. No email or other communications shall be sent which attempts to hide the identity of the sender, which may conceal information which is subject to the Government Records Act, or misrepresent the sender.

8. Users shall not reveal their passwords or other proprietary information, i.e. IP addresses, server names, etc. without a business necessity.

C. Use of Telephones
All county owned telephones, including cell phones shall be considered electronic communication. Personal long distance/toll calls should not be charged to the County at any time.

D. Social Media
Departments and/or employees that use social media for official County purposes are responsible for complying with applicable federal, state, and local laws, regulations and policies, including these Personnel Policies. Use of social media shall follow the guidelines established by Summit County. No employee shall use personal social media in a manner which implies official County participation, uses documents or images obtained as part of their employment, or in a manner which is illegal, violates County policies or is contrary to the County’s lawful interests.
E. **Use of Electronic Mail**

1. Generally
   a. Do not amend any messages received and, except where specifically authorized by the other person, do not access any other person's in-box or other email folders nor send any email purporting to come from another person.
   
b. It is good practice to re-read and check an email before sending, including using a spell checking or grammatical checking program.

2. Business use
   a. Each county email should be sent using the county email system and server and not from any personal account.
   
b. If the email message or attachment contains information which is time-critical, bear in mind that an email is not necessarily an instant communication and consider whether it is the most appropriate means of communication.
   
c. It may be appropriate to file a hard copy of any email (including any attachments) sent to or received, to a paper file for use and viewing by others. The same applies to all internal email transmissions concerning county matters. Each Department Head may determine the appropriateness of this action.
   
d. All email shall be retained pursuant to the State of Utah retention schedule found at http://archives.utah.gov/recordsmanagement/erm/email-guidelines.pdf

3. Personal Use
   a. Electronic communication has been established for County business use and should not be used for personal, outside business or employment, or non-County related purposes. However, limited, occasional, or incidental use of electronic communications for personal, non-County purposes, is acceptable insofar that the use complies with County policy, does not interfere with the County's business activities, and as long as such use does not involve any of the following:

   1) Interference with existing County rules or policies;
   2) Disrupt or distract from the conduct of County business;
   3) Solicitation;
   4) A for profit personal business activity;
   5) Potential to harm the County;

Section 18 Page 3
6) Illegal activities;

7) The display, storage or recording any kind of nude, obscene, pornographic, sexually explicit or other image or document intended to appeal to a prurient interest in sex.

   a. Personal email sent by employees using county email systems shall be retained in a separate email folder marked "Personal" should the employee wish to retain it after reading. Contact IT if you need guidance on how to set up and use a personal folder. All email contained in your inbox and your sent items box is deemed to be business communications.

Employees must ensure that personal email use:

1) Does not interfere with the performance of assigned duties;

2) Does not take priority over assigned work responsibilities;

3) Is minimal and limited to taking place substantially outside of normal working hours (i.e. during any breaks which the employee may be entitled to or before or after normal hours of work);

4) Does not cause unwarranted expense or liability to be incurred by Summit County;

5) Does not have a negative impact on Summit County in any way;

6) Is lawful and complies with this policy.

   c. Employees may delete personal email from the email system and are not required to follow any retention schedule. However, employees should know that backups may exist on the server and as such will be retained by the County.

   d. Employees shall be responsible for any charges arising from personal use of electronic communication services. Employees are expected to act responsibly and shall be subject to disciplinary action if this privilege is abused. By making personal use of county email systems, employees agree to abide by the conditions imposed for their use.

F. **Use of Internet and Intranet**

1. Employees shall not attempt to circumvent any filtering or content control of the internet and acknowledge that when visiting a website, information identifying your PC may be logged.

2. The internet and intranet shall be used for legitimate County purposes. Limited personal use is permitted subject to the same rules as are set out for personal email use in section C of this policy. If personal use requires additional software to be installed onto your PC or other device, employees should submit a request
to IT and receive approval before installing or connecting the device to county networks. This policy would carry over to any contract employee of Summit County which uses personal equipment while on county sites or connected to county resources.

3. Employees should not use their county email address when using public websites for non-county purposes, such as online shopping.

4. Any employee who may require access to websites generally blocked by Summit County as part of their duties (e.g. law enforcement) shall make the request to IT and shall have the express consent of the Department Head.

Employees shall not:

a. Introduce packet-sniffing or password-detecting software;

b. Seek to gain access to restricted areas of Summit County's network or access files for which they are not authorized;

c. Access or try to access data which the employee knows or should know is confidential;

d. Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software; nor

e. Carry out any hacking activities;

f. Participate in any internet chat room or post messages on any external website, including any message board or blog.

G. Misuse of Summit County Equipment and Systems

1. Misuse of Summit County equipment and systems, including its telephone, email and internet systems, in breach of this policy will be treated seriously. In particular, viewing, accessing, transmitting, posting, downloading or uploading any of the following materials in the following ways, or inappropriate use of any of Summit County equipment may subject the offending employee to discipline up to and including termination:

a. Material which is sexist, racist, homophobic, xenophobic, pornographic, pedophilic or similarly discriminatory and/or offensive;

b. Offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to Summit County or bring the reputation of Summit County and any of its elected officials or staff into disrepute;

c. Any defamatory material about any person or organization or material which includes statements which are untrue or of a deceptive nature;

d. Any material which, by intent or otherwise, harasses the recipient;
e. Any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;

f. Any material which violates the privacy of others or unfairly criticizes or misrepresents others;

g. Confidential information about an employee of Summit County;

h. Any other intentional statement which is likely to create any liability (whether criminal or civil) for Summit County;

i. Material in breach of copyright and/or other intellectual property rights;

j. Any subversive statement or activity which seeks to undermine the authority or purpose of Summit County or any other federal, state or local governmental entity.

k. Online gambling; or

l. Unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

H. System Security

1. Security of Summit County systems is of paramount importance. As a governmental entity, the County owes a duty to the public to ensure that all transactions are kept confidential where required and free of outside interference. If at any time the County needs to rely in court on any information which has been stored or processed using county IT systems it is essential to demonstrate the integrity of those systems. Employees using the system take responsibility for the security implications surrounding their acts.

2. County systems or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

3. Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorized third party.

4. Employees should keep system passwords safe. Do not disclose them to anyone. In the event assistance from IT is needed, a password change will be required.

5. Employees should not download or install software from external sources without having first received the necessary authorization from the IT department.

6. Employees should always exercise caution when opening emails from unknown external sources or where, for any reason, an email appears suspicious. The IT department should be informed immediately in such circumstances.
I. Working Remotely

1. This policy applies to the use of County systems, on County owned laptops, tablets or other devices as well as employee owned computer equipment or other computer equipment whenever employees may use them when working on County business away from the regular office environment (working remotely).

   Employees who may work remotely must:

   a. Password protect any work which relates to County business so that no other person can access the employee’s work;

   b. Position themselves so that work cannot be seen by any other person;

   c. Take reasonable precautions to safeguard the security of County equipment, and keep passwords secret;

   d. Inform law enforcement and the IT department (as appropriate) as soon as possible, but in any event no later than 24 hours after the fact, if any County owned equipment, has been lost or stolen; and

   e. Ensure that any work done remotely is saved on the County system or is transferred to our system as soon as reasonably practicable.

   1. Pocket computers, mobile phones and similar hand-held devices, external storage devices, and any internet based storage (cloud) are easily lost, stolen, or compromised, so employees must password-protect access to any such devices or services used by the employee.

      a. Employees should not be in the practice of storing information produced as a county employee on a personal device or internet storage without giving access to the employee’s supervisor, County Attorney, or the IT Department.

J. Personal Social Media, Blogs and Websites

1. This part of the policy and procedures in it apply to personal non-county content published on the internet even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.

2. Summit County recognizes that employees may wish to publish content on the internet on their private time. Those activities should remain in the realm of private time and should not be done during regular working hours.

3. Employees who post any content to the internet, written, vocal or visual, which identifies, or could identify, them as a member of Summit County staff and/or who discusses County work or anything related to Summit County or its business, elected officials or staff shall be expected, at all times, to conduct themselves appropriately and in a manner which is consistent with the County’s Personnel Policies and Procedures. It should be noted that simply revealing name or a visual image of the employee could be sufficient to identify them as an individual who works for Summit County.
4. If an internet posting clearly identifies that the employee works for Summit County and expresses any idea or opinion which is not authorized by the County then a disclaimer such as "these are my own personal views and not those of Summit County" must be added.

5. The following matters shall be treated as gross misconduct capable of resulting in immediate termination.
   a. Revealing confidential information obtained through employment with the County that would be considered protected or private as defined by the GRAMA statutes.
   b. Information which would be considered criminal whether or not formal charges are filed.
   c. Any information, photos or writing in which Summit County is identified and which is pornographic or obscene in nature.

6. Online publications which do not identify the author as an employee of the County and do not mention Summit County and are purely concerned with personal matters will normally fall outside the scope of this communications policy.

K. Privacy and Monitoring of Communications
   1. Electronic information created and/or communicated using e-mail, word processing, utility programs, spreadsheets, voice mail, telephones, fax machines, electronic communication access, etc. is randomly monitored by the County. County personnel are on notice of the following:
      a. The County routinely monitors usage patterns for both voice and data communications for cost analysis and electronic communication management (i.e., number called or site accessed, call length, call frequency, etc.)
      b. All electronic information on county owned equipment is the property of the County, and users shall not have an expectation of privacy in this regard. This includes but it not limited to data, facsimiles, texts, pictures, e-mail and voice mail files. Employees should not assume electronic communications are private and confidential and should transmit private and sensitive information in other ways.
      c. The display of any kind of image or document on any County system which is sexually explicit, obscene, and pornographic or which is designed to appeal to the prurient interest in sex is a violation of the County’s policy on sexual harassment. In addition, sexually explicit material shall not be archived, stored, distributed, edited or recorded using the County’s network or computing resources.
      d. The County reserves the right, at its discretion, to review any user’s electronic files/messages and usage to the extent necessary to ensure that electronic communication devices and services are being used in
compliance with the law and County policy and may disclose the contents of any user's electronic files/messages and usage of electronic media and services for a business or legal purpose.

e. The County may use independently supplied software and data to identify inappropriate or sexually explicit electronic communication sites. The County may block access from its networks to all such sites that it knows of. If an employee becomes connected accidentally to a site that contains sexually explicit or offensive material, the employee must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. The employee must also report that connection to the I.T. Department who shall keep a list of such reports.

1) Authorized law enforcement and prosecution representatives may, when approved by their department heads, access sexually explicit Internet sites during the course of a law enforcement investigation or prosecution.

f. The County’s electronic communication facilities and computing resources may not be used to knowingly violate the laws and regulations of the United States or the laws and regulations of any state, county, city or other local jurisdiction in any material way. Use of any County resources for illegal activity is grounds for immediate dismissal and the County will cooperate with any legitimate law enforcement agency.

g. The County may restrict a user's time allotment for using electronic communication devices for business purposes should such use be excessive or extravagant.

h. Anyone obtaining electronic access to other organizations' or individuals' material must respect all applicable laws and shall not copy, retrieve, modify, or forward copyrighted materials except as expressly permitted by the copyright owner.

i. Electronic communication access and usage by a County employee will be allowed only upon the approval of the employee's department head.

K. Compliance with this Policy
The provision of electronic communication devices and services are at the discretion of the County and are a revocable privilege. Any County employee found to be abusing the privilege of County facilitated access to electronic communication devices or services shall be subject to disciplinary action up to and including dismissal.
Tab 12
User Rules of Behavior Acknowledgment Form

As a user of an IT system, I acknowledge my responsibility to conform to the following requirements and conditions as directed by all relevant Information Assurance and Information Security Policies, Procedures and Guidelines. These conditions apply to all personnel who have access to FBI CJIS systems and all appropriate IT personnel.

1. I understand that failure to sign this acknowledgment will result in denial of access to FBI CJIS systems, terminal areas, and facilities that have FBI CJIS network equipment.

2. I acknowledge my responsibility to use the network only for official business except for such personal use involving negligible cost to the agency and no interference with official business as may be permissible under the acceptable use policy.

3. I understand that the network operates at a Sensitive but Unclassified level. I have all clearance necessary for access to the network, and will not introduce or process data that the network is not specifically designed to handle as specified by the Security Policy.

4. I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account. I understand that neither the Security Administrator/System Administrator, nor the Network Operations Center (NOC) will request my password. I will change my password at least every 90 days or as requested for security reasons.

5. I understand I am responsible for all actions taken under my account. I will not attempt to "hack" the network or any connected automated information system (AIS), or attempt to gain access to data for which I am not specifically authorized.

6. I understand my responsibility to appropriately protect all output generated under my account, to include printed material, magnetic tapes, floppy disks, CD-ROMs, and downloaded hard disk files. I understand that I am required to ensure all hard copy material and magnetic media is properly labeled as required by policies and regulations.

7. I understand my responsibility to report all AIS or network problems to my security point of contact. I will NOT install, remove, or modify any hardware or software.
8. I acknowledge my responsibility to not introduce any software or hardware not acquired and approved through the IT Security group. I also acknowledge my responsibility to have all official electronic media virus-scanned by the IT Security group before introducing it into the AIS or network.

9. I acknowledge my responsibility to conform to the requirements of the Rules of Behavior, Acceptable Use Policy, and Security Policies and Procedures. I also acknowledge that failure to comply with these policies and procedures may constitute a security violation resulting in denial of access to the AIS, network, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.

10. I agree that I have no expectation of privacy in any equipment or media I use. I consent to inspections by authorized agency personnel, at any time and agree to make any equipment available for audit and review by FBI personnel upon request.

11. I further consent that my use of FBI CJIS systems within agency owned or leased space is subject to system monitoring.

12. I have completed the required triennial Security Awareness Training required by the CJIS Security Policy for individuals managing or accessing FBI CJIS systems and/or data.

User (Print Name): ____________________________ Date: ______________

User Signature: ______________________________ Date: ______________

ISO/Security Officer: __________________________ Date: ______________
Disposal of Media Policy and Procedures

1.0 Purpose
The purpose of this policy is to outline the proper disposal of media (physical or electronic) at [Agency Name]. These rules are in place to protect sensitive and classified information, employees and [Agency Name]. Inappropriate disposal of [Agency Name] and FBI Criminal Justice Information (CJI) and media may put employees, [Agency Name] and the FBI at risk.

2.0 Scope
This policy applies to all [Agency Name] employees, contractors, temporary staff, and other workers at [Agency Name], with access to FBI CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by [Agency Name].

3.0 Policy
When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by [Agency Name].

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

1) shredding using [Agency Name] issued shredders.

2) placed in locked shredding bins for [private contractor name] to come on-site and shred, witnessed by [Agency Name] personnel throughout the entire process.

3) incineration using [Agency Name] incinerators or witnessed by [Agency Name] personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the <Agency Name> methods:

1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

2) **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

3) **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from [Agency Name]'s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.
4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.
Purpose:
All accounts shall be reviewed at least every six months by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges are commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.

All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The TAC must disable all new accounts that have not been accessed within 30 days of creation.

Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC must be notified if a user’s information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual’s account(s) to the new office (CJA).

The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC).

The TAC shall:
- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
- Periodically review existing accounts for validity (at least once every 6 months), and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.
Purpose:
The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

This Physical Protection Policy was developed using the FBI's CJIS Security Policy 5.1 dated July 13, 2012. The intended target audience is [agency name] personnel, support personnel, and private contractor/vendors with access to CJI whether logically or physically. The local agency may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Physically Secure Location:
A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the [agency name] shall be identified with a sign at the entrance.

Visitors Access:
A visitor is defined as a person who visits the [agency name] facility on a temporary basis who is not employed by the [agency name] and has no unescorted access to the physically secure location within the [agency name] where FBI CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.
Visitors shall:

1. Check in before entering a physically secure location by:
   a. Completing the visitor access log, which includes: name and visitor’s agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
   b. Document badge number on visitor log if visitor badge issued. If [agency name] issues visitor badges, the visitor badge shall be worn on approved visitor’s outer clothing and collected by the agency at the end of the visit.
   c. Planning to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has their own individual perimeter security to protect CJI.

2. Be accompanied by [agency name] escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

3. Show [agency name] personnel a valid form of photo identification.

4. Follow [agency name] policy for authorized unescorted access.
   a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the [agency name] and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.
   b. Private contractors/vendors who requires frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the [agency name] and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

5. Not be allowed to view screen information mitigating shoulder surfing.

6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

7. Not be allowed to sponsor another visitor.

8. Not enter into a secure area with electronic devices unless approved by the [agency name] Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the [agency name] assigned personnel.

9. All requests by groups for tours of the [agency name] facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.
Authorized Physical Access:
Only authorized personnel will have access to physically secure non-public locations. The [agency name] will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:
1. Meet the minimum personnel screening requirements prior to CJI access.
   a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
   b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
   c. Prior to granting access to CJI, the [agency name] on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.
   d. Refer to the CIIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete security awareness training.
   a. All authorized [agency name], Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
   b. Security awareness training will cover areas specified in the CIIS Security Policy at a minimum.
3. Be aware of who is in their secure area before accessing confidential data.
   a. Take appropriate action to protect all confidential data.
   b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
   a. Report loss of issued keys, proximity cards, etc to authorized agency personnel.
   b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the [agency name] POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.
   c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.
5. Properly protect from viruses, worms, Trojan horses, and other malicious code.
6. Web usage—allowed versus prohibited; monitoring of user activity. (allowed versus prohibited is at the agency’s discretion)


8. Use of electronic media is allowed only by authorized [agency name] personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

9. Encrypt emails when electronic mail is allowed to transmit CJI-related data as such in the case of Information Exchange Agreements.
   a. (Agency Discretion for allowance of CJI via email)
   b. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.

10. Report any physical security incidents to the [agency name]’s LASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.

11. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed.
    Information should be shared on a “need to know” basis. (See Sanitization and Destruction Policy)

12. Ensure data centers with CJI are physically and logically secure.

13. Keep appropriate [agency name] security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.

14. Not use food or drink around information technology equipment.

15. Know which door to use for proper entry and exit of the [agency name] and only use marked alarmed fire exits in emergency situations.

16. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

Roles and Responsibilities:

Terminal Agency Coordinator (TAC)
The TAC serves as the point-of-contact at the [agency name] for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency’s compliance with FBI and state CJIS systems policies.

Local Agency Security Officer (LASO)
Each LASO shall:
1. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.
Agency Coordinator (AC)
An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the [agency name]. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCIA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

CJIS System Agency Information Security Officer (CSA ISO)
The CSA ISO shall:
1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA’s user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

Information Technology Support
In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the [agency name] by performing the following:
1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the [agency name]. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required [agency name] technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI-based terminals, servers, switches, etc.
4. Properly protect the [agency name]’s CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
   a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the [agency name] allows the use of personally owned devices. (See the [agency name] Personally Owned Device Policy)

5. Data backup and storage—centralized or decentralized approach.

a. Perform data backups and take appropriate measures to protect all stored CJI.

b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured location.

c. Ensure any media released from the [agency name] is properly sanitized / destroyed. (See Sanitization and Destruction Policy)

6. Timely application of system patches—part of configuration management.

a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

b. When applicable, see the [agency name] Patch Management Policy.

7. Access control measures

a. Address least privilege and separation of duties.

b. Enable event logging of:

   i. Successful and unsuccessful system log-on attempts.

   ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.

   iii. Successful and unsuccessful attempts to change account passwords.

   iv. Successful and unsuccessful actions by privileged accounts.

   v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

8. Account Management in coordination with TAC

a. Agencies shall ensure that all user IDs belong to currently authorized users.

b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.

c. Authenticate verified users as uniquely identified.

d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.

e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.

f. Passwords

   i. Be a minimum length of eight (8) characters on all systems.

   ii. Not be a dictionary word or proper name.

   iii. Not be the same as the Userid.

   iv. Expire within a maximum of 90 calendar days.
v. Not be identical to the previous ten (10) passwords.
vi. Not be transmitted in the clear or plaintext outside the secure location.
vii. Not be displayed when entered.
viii. Ensure passwords are only reset for authorized user.

   a. Take action to protect CJI-related data from unauthorized public access.
   b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
   c. Enable and update personal firewall on mobile devices as needed.
   d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and *advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. *Note: for interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.
   e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
   f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
   g. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the [agency name]. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

10. Communicate and keep the [agency name] informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to [agency name].

Front desk and Visitor Sponsoring Personnel
Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility. In most facilities, this duty is done by the Front desk or Reception Desk.

Prior to visitor gaining access to physically secure area:
1. The visitor will be screened by the [agency name] personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the [agency name].
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the [agency name].
3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.
4. Escort and/or Front desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

All [agency name] personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the [agency name] officials. For [agency name], the point of contacts to report any non-secure access is:

<table>
<thead>
<tr>
<th>LASO Name:</th>
<th>LASO Phone:</th>
<th>LASO email:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Name:</td>
<td>AC Phone:</td>
<td>AC email:</td>
</tr>
<tr>
<td>State C/ISO Name:</td>
<td>C/ISO Phone:</td>
<td>C/ISO email:</td>
</tr>
</tbody>
</table>

Penalties:
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

Acknowledgement:
I have read the policy and rules above and I will:
- Abide by the [agency name] Physical Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect the [agency name]'s facilities, personnel and associated information systems.
- Report any unauthorized physical access to the [agency name]'s LASO.

Signature: ______________________________ Date: ____________ /2012__

Other Related Policy Reference:
- Sanitization and Destruction Policy
- Disciplinary Policy
- CIJS Security Policy
Policy Title: Allowed Personally Owned Device Policy

Effective Date:

Revision Date: Every 2 years or as needed

Approval(s):

LASO:

CSO:

Agency Head:

Purpose:
A personally owned information system or device shall be authorized to access, process, store or transmit [agency name], state, or FBI Criminal Justice Information (CJI) only when these established and documented specific terms and conditions are met. This control does not apply to the use of personally owned information systems to access the [agency name]'s information systems and information that are intended for public access (e.g., an agency’s public website that contains purely public information).

This Personally Owned Device Policy was developed using the FBI’s CIJS Security Policy 5.1 dated July 13, 2012. The intended target audience is [agency name] personnel, support personnel and private contractors/vendors. The [agency name] may complement this policy with a local policy; however, the CIJS Security Policy shall always be the minimum standard and the local policy may augment, or increase the standards, but shall not detract from the CIJS Security Policy standards.

Scope:
This policy applies to all [agency name] personnel, support personnel, and/or private contractors/vendors who are authorized to use personally owned devices to connect to any physical, logical, and/or electronic premise of the [agency name] to access, process, store, and/or transmit CJI. This also includes any private contractors/vendors who will conduct maintenance on any network device that processes, stores, and/or transmits FBI CJI.

Personally Owned Devices:
A personally owned device is any technology device that was purchased by an individual and was not issued by the [agency name]. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. Threats to mobile handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

The [agency name] will maintain management control and authorize the use of personally owned devices. The [agency name] shall develop guidelines to define which
employees can use their own devices, the types of devices they can use, and which applications and data they can access, process, or store on their devices.

Personally owned devices must:
- Be authorized by [agency name] to access, process, transmit, and/or store FBI CJI.
- Be inspected by [agency name]'s IT staff and the LASO to ensure appropriate security requirements on the device are up-to-date and meet the FBI’s CIJS Security Policy requirements prior to use.
- Take necessary precautions when using device outside of a physically secure area. Read below and also see Physical Protection Policy.

Remote Access:
The [agency name] shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency’s information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The [agency name] shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The [agency name] shall control all remote accesses through managed access control points. The [agency name] may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Roles and Responsibilities:

Owner Role: The owner agrees to:
1. Follow necessary policy and procedures to protect FBI CJI.
2. Usage of their device will be for work-related purposes.
3. Bring their device to work to use during normal work hours and not share the device with anyone else.
4. [agency name] having the authority to erase device remotely as needed.
5. Be responsible for any financial obligations for device.
6. Protect individual’s and [agency name]'s privacy.
7. Use good judgement before installing free applications. Sometimes free applications track your personal information with limited disclosure or authorization, and then sell your profile to advertising companies.
8. Use good judgement on amount of time applied to personal use of personally owned devices during normal work business hours.
9. Access FBI CJII only from an approved and authorized storage device.
10. Do not stream music or videos using personally owned devices when connected to [agency name]'s network to prevent sluggishness.
11. Report lost or stolen mobile or storage devices to the [agency name]'s Local Agency Security Officer (LASO) within one business day.
12. Review the use of device alerts and update services to validate you requested them. Restrict notifications not requested by looking at your device’s settings.
13. Control wireless network and service connectivity. Validate mobile device default settings are not connecting to nearby Wi-Fi networks automatically. Some of these networks, like in airports or neighborhood coffee shops, may be completely open and unsecure.

Information Technology Role
The [agency name] IT support role shall, at a minimum, ensure that external storage devices:
1. Are encrypted when FBI CJII is stored electronically.
2. Are scanned for virus and malware prior to use and/or prior to being connected to the agency’s computer or laptop.

The [agency name] IT support role shall, at a minimum, ensure that all personally owned devices:
1. Apply available critical patches and upgrades to the device operating system.
2. Are kept updated with security patches, firmware updates and antivirus.
3. Are configured for local device authentication.
4. Use advanced authentication and encryption when FBI CJII is stored and/or transmitted.
5. Be able to deliver built-in identity role-mapping, network access control (NAC), AAA (Authentication, Authorization, and Accounting) services, and real-time endpoint reporting.
6. Erase cached information when session is terminated.
7. Employ personal firewalls.
8. Minimize security risks by ensuring antivirus and antimalware are installed, running real time and updated.
9. Be scanned for viruses and malware prior to accessing or connecting to [agency name] CJIS network.
10. Configure Bluetooth interface as undiscoverable except as needed for pairing, which prevents visibility to other Bluetooth devices except when discovery is specifically needed.
11. Be properly disposed of at end of life. See Media Disposal Policy. Remove FBI CJII before owner sells their personally owned devices or sends it in for repairs.
12. Evaluate personally owned device age. Older device hardware is too outdated for needed updates. Typical life is two years.
13. Ensure device is compatible with needed network protocols and/or compatible with customized applications developed for access FBI CJI through testing.

14. Deploy Mobile Device Management or SIM card locks and credential functions. The credential functions require a pass code to use [agency name]'s network services. (*Research enterprise mobile device management solutions - see product working successfully in real life scenario with the type of mobile device your State/Agency wants to use prior to implementing. The enterprise mobile device solution must be compatible with chosen device products.*)

15. Ensure owner and IT staff have mobile backup enabled to an approved [agency name] location. Set a daily or weekly schedule to periodically synch data and applications. If backup contains FBI CJI, take appropriate security measures for storage of FBI CJI. See Media Protection Policy.

16. Retain the ability to secure, control and remotely erase agency data on employee-owned devices in the event of a security breach or if the employee leaves the agency employment or the device is lost or stolen. This remote ability can be done through technology that allows virtual access to company applications.

17. Enable mobile device in a “find my phone” service to allow finding device.

18. Consider adding extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of attempts.

19. Be able to easily identify connected users and devices. Track, log and manage every personally used device allowed to connect to agency technology resources for secure FBI CJI access.

20. Perform pre and post-authentication checks.

21. Ability to allow and deny access. Selectively grant proper network access privileges.

Local Area Security Officer (LASO)
The LASO will:

1. Identify who is using the personally owned approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

2. Identify and document how the equipment is connected to the state system.

3. Ensure that personnel security screening procedures are being followed as stated in this policy.

4. Ensure the approved and appropriate security measures are in place and working as expected.

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

Penalties:
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination. Personally owned information technology
<Criminal Justice Agency Name> Personally Owned Device Policy

resources used may be retained by the [agency name] for evaluation in investigation of security violations.

Violation of any of the requirements in this policy by any unauthorized person can result in similar disciplinary action against the device owner, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

Acknowledgement:
The [agency name], agency personnel, IT support, private contractors/vendors, and the LASO alike will agree to commit to all bring your own (BYO) rules.

I have read the policy and rules above and I will:
- Authorize the [agency name] to remotely wipe my mobile device.
- Abide by the [agency name] Personally Owned Device policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect [agency name] facilities, personnel and associated information systems.
- Report any unauthorized device access to [agency name] LASO.

Signature: _____________________________ Date: __________/20____

Questions
Any questions related to this policy may be directed to the [agency name]'s LASO:

<table>
<thead>
<tr>
<th>LASO Name:</th>
<th>LASO Phone:</th>
<th>LASO email:</th>
</tr>
</thead>
<tbody>
<tr>
<td>State CSO/ISO Name:</td>
<td>CSO/ISO Phone:</td>
<td>CSO/ISO email:</td>
</tr>
</tbody>
</table>

Other Related Policy Reference:
- See Media Sanitization and Destruction Policy
- Physical Protection Policy
<Criminal Justice Agency Name> Media Protection Policy

<table>
<thead>
<tr>
<th>Policy Title:</th>
<th>Media Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
<td></td>
</tr>
<tr>
<td>Revision Date:</td>
<td>Every 2 years or as needed</td>
</tr>
<tr>
<td>Approval(s):</td>
<td></td>
</tr>
<tr>
<td>LASO:</td>
<td></td>
</tr>
<tr>
<td>CSO:</td>
<td></td>
</tr>
<tr>
<td>Agency Head:</td>
<td></td>
</tr>
</tbody>
</table>

Purpose:
The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This Media Protection Policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.1 dated 7/13/2012. The [agency name] may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope:
The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the [agency name]. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized [agency name] personnel shall protect and control electronic and physical CJI while at rest and in transit. The [agency name] will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the [agency name] Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

Media Storage and Access:
Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. “Electronic media” includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” includes printed documents and imagery that contain CJI.
To protect CJI, the [agency name] personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)
5. Not use personally owned information system to access, process, store, or transmit CJI unless the [agency name] has established and documented the specific terms and conditions for personally owned information system usage. (See Personally Owned Device Policy)
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the [agency name] in a secure area accessible to only those employees whose job function require them to handle such documents.
8. Safeguard all CJI by the [agency name] against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
9. Take appropriate action when in possession of CJI while not in a secure area:
   a. CJI must not leave the employee’s immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
   b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and/or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
      i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
      ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
<Criminal Justice Agency Name> Media Protection Policy

10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.

11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

Media Transport:
Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:
1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The [agency name] personnel shall:
1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The [agency name] personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:
1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
   a. Storing CJI in a locked briefcase or lockbox.
   b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
   c. For hard copy printouts or CJI documents:
      i. Package hard copy printouts in such a way as to not have any CJI information viewable.
      ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI

Approved By: Agency Name Management
<Criminal Justice Agency Name> Media Protection Policy

material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)

5. Not taking CJI home or when traveling unless authorized by [agency name] LASO. When disposing confidential documents, use a shredder.

Electronic Media Sanitization and Disposal:
The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to “Sanitization Destruction Policy”.

Breach Notification and Incident Reporting:
The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Roles and Responsibilities:
If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. [agency name] personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)

2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.

3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.

4. The CSA ISO will:
   a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
<Criminal Justice Agency Name> Media Protection Policy

b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.

c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

Penalties:
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Acknowledgement:
I have read the policy and rules above and I will:
- Abide by the [agency name]'s Media Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Report any [agency name] CJI security incident to Supervisor and / or LASO as identified in this policy.

Signature: ___________________________ Date: __________/2012____

Questions
Any questions related to this policy may be directed to the [agency name]'s LASO:

<table>
<thead>
<tr>
<th>LASO Name:</th>
<th>LASO Phone:</th>
<th>LASO email:</th>
</tr>
</thead>
<tbody>
<tr>
<td>State C/ISO Name:</td>
<td>C/ISO Phone:</td>
<td>C/ISO email:</td>
</tr>
</tbody>
</table>

Other Related Policy Reference:
- See Media Sanitization and Destruction Policy
- Media Disposal Policy
- Physical Protection Policy
Information Technology Policy

POLICY 604-01: CYBER SECURITY INCIDENT RESPONSE

An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

OBJECTIVE:
Ensure the organization is prepared to respond to cyber security incidents, to protect State systems and data, and prevent disruption of government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

SCOPE:
This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of

RESPONSIBILITIES:

Individual Information Technology User:
All users of State of computing resources shall be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

Information Services Division (ISD):
Provide incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of ISD information systems. Incident response support resources may include, for example, the ISD Help Desk, a response team (described below), and access to forensics services.

Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. The CSIRT shall consist of members of the State IT Security Council and key personnel from other agencies as required. CSIRT responsibilities shall be defined in the Cyber Security Incident Reporting Procedures.

Agency Management, Information Technology Organization:
Develop organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.

Organizations that support information systems shall develop incident response plans and/or procedures that:

- Provides the organization with a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability
- Provides a high-level approach for how the incident response capability fits into the overall organization
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
- Defines reportable incidents

Policy 604-01: Incident Response
- Provides metrics for measuring the incident response capability within the organization
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Is reviewed and approved by designated officials within the organization

Review incident response plans and procedures at least annually.

Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.

Distribute copies of the incident response plan/procedures to incident response personnel.

Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.

Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.

Organizations shall test the incident response capability for the information systems they support at least annually. Use organization-defined tests and/or exercises to determine incident response effectiveness. Document the results.

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Coordinate incident handling activities with contingency planning activities.

Incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises.

Track and document information system security incidents. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Organizations that support information systems shall provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

**ADDITIONAL INFORMATION:**

Information Technology Procedure 604P1: Cyber Security Incident Reporting

Information Technology Procedure 604P2: Cyber Security Incident Handling
http://cybersecurity.alabama.gov/documents/Procedure_604P2_Incident_Handling.pdf

Information Technology Dictionary

*By Authority of Director, Information Services Division, Department of Finance*
Discussion regarding Summit County/North Summit Fire Reserve Wildland Firefighter policy; Ken Smith, Jami Brackin, and Brian Bellamy

Ken Smith, North Summit Fire Chief, Jami Brackin, Deputy Attorney, and Brian Bellamy, Personnel Director, met with the Council to propose a policy to allow certain county employees to be trained and serve as Reserve Wildland Firefighters.
Staff Report

To: Summit County Council
Date: December 24, 2018
From: Jami Brackin & Brian Bellamy
Subject: New Policy

A. Background

During the summer of 2018, the County experienced wild fires along I-80 among other areas. It was proposed if we had wildland fire trained County Employees, who work in the North Summit County area, respond to these fires, the fires may have been knocked down quicker than waiting for other wildland firefighters to get to the site.

In conversations with Ken Smith, North Summit Fire District Chief and Paul Hewitt, Park City Fire District Chief it was agreed it would be a useful to train a few county employees as Reserve Wildland Firefighters. Chief Hewitt stated he most likely would not use these employees, due to the pool of experienced firefighters he has available to him, but Chief Smith thought it was a great idea.

Knowing the employees would need to be trained and educated to work on how to fight wildland fires, the County developed the attached policy. Under this policy, up to ten county employees will be permitted to participate. Each employee will be required to obtain their Department Head or Elected Official's approval; no more than two employees from the same department shall be allowed to participate. The department head may deny the employee's request to be included in fighting wildland fires, if the department's workload would be adversely impacted or if the department already has two employees from the department involved.

This policy also requires the employee to be paid their regular County pay rate. North Summit Fire District will reimburse Summit County the allowed Wildland Firefighter Type 2 pay rate from the cost recovery billing funds.
As written, the policy also requires the County employees to be the first released from any wildfire fighting activity.

The purpose of the attached policy is to address the need in helping fight wildland fires. This policy will also increase the wildland firefighter pool in the North Summit area.

No County employee functioning as a Reserve Wildland Firefighter will be permitted to fight a structure fire.

This policy has been previously reviewed by Summit County Manager Tom Fisher.

B. **Recommendations**

1. We recommend you review the attached policy.
2. We recommend if you would like a work session on the proposed policy you notify one of the authors by January 5, 2019. If you choose not to hold a work session this policy will be forwarded to Tom Fisher, Summit County Manager, for approval by Executive Order.
3. Upon approval of this policy, Human Resources will send notification of approval to all department heads and elected officials. This policy will also be sent to all employees and placed on the Summit Buzz.
Summit County/North Summit Fire
Reserve Wildland Firefighter

A. To enhance response time and increase the number of firefighters available to the North Summit Fire District, Summit County authorizes up to ten County employees to be educated and trained to act as Reserve Wildland Firefighters.

1. A Summit County Reserve Wildland Firefighter will serve on a hand crew or engine crew, performing fire suppression and fuels management duties in the most adverse climate, fuel, and terrain conditions.

2. The County Reserve Wildland Firefighter has no supervisory responsibilities and shall be supervised by an experienced Firefighter or one of the Single Resource Bosses.

3. Duties involve fieldwork requiring physical performance calling for above-average endurance and superior conditioning. These duties may include an occasional demand for extraordinarily strenuous activities in emergencies under adverse environmental conditions and over extended periods of time.

   a. Due the strenuous nature of this work all applicants shall provide, at the time of application, proof they have recently passed a similar test as listed in sub-paragraph 5 below or provide a doctor’s note stating they are physically fit and can participate in strenuous activities.

4. Will receive all necessary education to be qualified as a Wildland Firefighter Type 2.

   a. Must pass Wildland Firefighter classes.

5. Must pass a physical fitness test. The test may consist of a 3-mile hike with a 45-pound pack over level terrain. A time of 45 minutes, is the passing score for the test.

B. To mitigate the impact on Summit County Government Operations, applicants must first submit an approval form, signed by their Department Head/Elected Official. If the Department Head/Elected Official determines that an employee(s) serving as a Wildland Firefighter will adversely affect the department or office, the Department Head/Elected Official may choose to withhold permission.

1. If permission is withheld, the employee shall not participate as a Wildland Firefighter.

   a. There shall be no appeal of the Department Head/Elected Officials’ decision.
b. The employee may reapply in one year if current county employees (within the Department) are no longer functioning as Wildland Firefighters.

2. Salary
   a. If the employee is called to fight a wildland fire during their Summit County normal work schedule, the employee shall continue to be compensated at their regular rate of pay.

   b. If the employee is called out to fight a fire outside of their normal Summit County shift, they shall be compensated at their Summit County hourly rate.

   c. The North Summit Fire District shall reimburse the County from the cost recovery billing funds for a Wildland Firefighter Type 2 hourly rate while the Summit County employee is fighting a fire.

C. Responsibility of North Summit Fire District
   1. When fire suppression related circumstances allow, Summit County employee Wildland Firefighters shall be the first released from firefighting responsibilities.
Staff has begun a comprehensive review of the Snyderville Basin Development Code. A subcommittee was established consisting of members of Staff and the Planning Commission. The following list outlines the strategy moving forward envisioned by Staff.

**Code Amendments Recently Processed**

- Food Trucks: Approved
- Chapters 1 (Title, Authority, Purpose and Applicability) and Chapter 2 (User Guide): Recommended for approval by the Planning Commission on 10.9.18.

**Code Amendments Under Review**

- Lighting Ordinance
- Master Planned Development Process
- Neighborhood Mixed Use Zone
- Residential Zones, including uses and definitions

**Pending Code Amendments**

- Commercial Zones, including uses and definitions
- Development Review Processes (Subdivisions, Conditional Use Permits, Low Impact Permits, etc.)
- Sustainability (Landscaping, Solar, Recycling, etc.)

**Future Code Amendments**

- The remaining chapters of the Code will be reviewed. It is anticipated that the subcommittee will establish the order in which the remaining amendments should be reviewed.
The Council was supportive of this policy with a few clarifications. It could then be forwarded to Manager Fisher for approval by Executive Order.

County resident David Sime made comment on the definition of Reserve Wildland Firefighter if this was the correct definition. He also asked if they would be covered under workman’s compensation.

Council Member Carson thanked him for his comments.

Council Minutes dated December 5, 2018, December 6, 2018, December 10, 2018, December 12, 2018, and December 18, 2018

Council Member Wright made a motion to approve the minutes of December 5, December 6, December 10, December 12, and December 18, 2018 with one correction to the December 12 minutes noted. Council Member Carson seconded and all voted in favor, 3-0.

Council Comments

- Council Member Carson attended the Board of Health meeting. Discussion included medical cannabis and effects to the Health Department for funding, security, and training.

- Council Member Wright attended the TRUCE meeting discussing similar issues.
- He suggested a work session regarding Wildland Fire issues and resident’s participation for clean up around their homes.
- He attended the Mountainlands Community Housing meeting. Issues discussed include funding and climbing supply costs.

Manager Comments

There were no manager comments.

Public Input

There was no public input.

Joint meeting with Snyderville Basin Planning Commission to discuss work tasks and deadlines for 2019; Pat Putt

The Council met with members of the Snyderville Basin Planning Commission and Pat Putt, Community Development Director, to discuss work tasks and completion target dates for 2019. Council Member Robinson joined the discussion by phone.

The Council meeting adjourned at 7:56 p.m.

Roger Armstrong, Chair

Kellie Robinson, Chief Deputy Clerk