



Minutes
Sumter County Council
Regular Meeting
April 28, 2009 - Held at 6:00 p.m.
County Administration Building County Council Chambers
13 E. Canal Street, Sumter, SC

.....
COUNCIL MEMBERS PRESENT:

1. Chairman Vivian Fleming McGhaney, Council District #5
2. Vice Chairman Eugene Baten, Council District #7
3. Councilman Artie Baker, Council District #2
4. Councilman Larry Blanding, Council District #6
5. Councilman Jimmy Byrd, Council District #3
6. Councilman Charles T. Edens, Council District #4
7. Councilwoman Naomi D. Sanders, Council District #1

COUNCIL MEMBERS ABSENT: None

STAFF MEMBERS PRESENT:

William T. Noonan, County Administrator
Johnathan Bryan, County Attorney
Donna McCullum, Zoning Administrator
Lorraine Dennis, Deputy Administrator/HR
Keysa Rogers, Budget Analyst

Mary W. Blanding, Clerk To County Council
Peter Wilson, County Engineer
Gary Mixon, Deputy Administrator
Pam Craven, Finance Director
Henry Bailey, Planner

MEDIA PRESENT:

The Item Newspaper

THE PUBLIC PRESENT:

Approximately four members of the public were in attendance.

.....
CALL TO ORDER: Chairwoman Vivian Fleming McGhaney called Sumter County Council's meeting of April 28, 2009, to order.

INVOCATION: The Chairwoman, Vivian Fleming McGhaney, gave the invocation.

PLEDGE OF ALLEGIANCE: All in attendance repeated the Pledge of Allegiance.

APPROVAL OF AGENDA: Chairwoman McGhaney stated that she would entertain a motion to approve the April 28, 2009, agenda with any additions, deletions, or as printed.

ACTION: MOTION was made by Councilman Baker, seconded by Councilman Byrd, and unanimously carried by Council to approve the April 28, 2009, agenda as prepared by the Clerk.

ACTION ON REGULAR AND BUDGET MEETING MINUTES OF APRIL 14, 2009, AND APRIL 21, 2009: Chairwoman McGhaney stated that she would entertain a motion to approve the regular and Budget meeting minutes of County Council held on April 14, 2009, and April 21, 2009, respectively.

ACTION: MOTION was made by Councilman Baker, seconded by Councilman Byrd, and unanimously carried by Council to approve the April 14, 2009, and April 21, 2009, minutes of Council's regular and budget meeting as prepared by the Clerk.

INTRODUCTION: The Clerk introduced Mr. Drayton Ward, with Boy Scout Troop #86, he was accompanied with his father Mr. Daly Ward. Drayton Ward is working on his Eagle Scout Badge.

**LAND USE MATTERS AND REZONING REQUESTS -
Planned Development/Rezoning Request -**

- (1) OA-09-01 -- Third Reading -- Planning Staff (County) - (09-681) -- A Request To Amend Article 4, Section G; Article 3, Sections B, C, And D; And Article 10, Section B Of The County Zoning And Development Standards Ordinance Pertaining To The Size, Height, Location, Number, And Setbacks For Accessory Structures.

Mr. Henry Bailey, Planner, stated that there have been no changes to this ordinance amendment since first reading. Then Council took action on third reading.

ACTION: MOTION was made by Councilman Baker, seconded by Councilman Byrd, and unanimously carried by Council to grant third reading and adoption.

Street Name Change - None

Grant Awards -

OTHER PUBLIC HEARINGS -- None

NEW BUSINESS:

- (1) It May Be Necessary To Hold An Executive Session To Discuss A Personnel Matter, Receive A Legal Briefing, Or Discuss A Contractual Matter And Appropriate Actions May Be Required And Taken Thereafter.

No executive session was held.

OLD BUSINESS:

- (1) Third Reading -- 09-682 -- An Ordinance To Define And Prohibit Illicit Discharges And Connections To Storm Water Sewer Systems And Waters Of The State For Sumter County, South Carolina.

The County Attorney presented this proposed ordinance to Council for third reading consideration. After some discussion whether or not to defer or to take action on third reading, Council agreed to take action on the approval of third reading. (This matter was discussed thoroughly during the Fiscal, Tax, and Property Committee meeting held prior to this meeting.)

ACTION: MOTION was made by Councilman Baker, seconded by Vice Chairman Baten, and carried by Council to grant third reading and adoption. Council members Edens and Byrd voted in opposition. The motion carried.

COMMITTEE REPORTS:

- (1) Special Budget Workshop Held On Tuesday, **April 28, 2009, at At 4:00 P.M. In County Council's Conference Room At The County Administration Building -- All Council Members Are To Attend.**

The Administrator presented a synopsis of the budget meeting held on today. He stated that Council did not take any actions on this matter; however, he presented this information for the benefit of the public.

Budget projections as of April 14, 2009:

• Expenditures	\$47,143,184	
• Revenues		\$43,536,256
• Increase in Lease Payments	\$322,560	

Budget as of April 28, 2009

• Expenditures	\$47,465,744	
• Revenue		\$43,536,256
• Deficit		\$3,929,488

It was noted that the deficit does not include capital requests of \$2.1 million.

The County Administrator further provided Council members with additional budget options; the projections will be further discussed at a budget workshop scheduled for May 5, 2009.

ACTION: No action taken on this matter.

- (2) **Fiscal, Tax, and Property Committee Meeting Held On Tuesday, April 28, 2009, At 5:00 P.M. In County Council's Conference Room At The County Administration Building (Vivian Fleming McGhaney, Charles T. Edens, and Larry Blanding.) All Council Members Are Urged To Attend.**

The Chairwoman of the Committee, Vivian Fleming McGhaney, presented the following report and recommendations.

- **Identity Theft Prevention Policy (Red Flag)** - The County Attorney presented the Prevention Identity Theft Policy (See attached document.) to the Committee for review. After review of the policy, the Committee recommended approval and implementation of the policy for Sumter County.

ACTION: MOTION and a second were received from the Committee, and unanimously carried by Council to approve the implementation and adoption of the

Identity Prevention Theft Policy (Red Flag) for Sumter County, South Carolina as presented.

- **Census 2010 Partnership Agreement:** The Committee reviewed the Census 2010 Partnership Agreement which is a program to combine the strengths of local governments, community-based organizations, faith-based organizations, schools, media, businesses, and others, to ensure a complete and accurate Census 2010. It was noted that the Census Bureau will provide promotional materials, regular updates, and data assistance to partners to assist in the effort to have an accurate and thorough count. The Committee recommended approval of the agreement.

ACTION: MOTION and a second were received from the Committee, and unanimously carried by Council to approve the adoption of the Census 2010 Partnership Agreement as presented.

(3) Report From Council Members On Other Meetings, Trainings, and/or Conferences.

No report given.

MONTHLY REPORTS:

- Sumter County Statement of General Fund Ending March 31, 2009
- United States Senate - Town Meeting Schedule
- Census 2010
- Sumter Economic Development
- Sumter Little Theatre

ADMINISTRATOR'S REPORT:

- **Booking Through The New Computer Software:** The Administrator recognized Simon Major, the Sumter-Lee Regional Detention Center Director, and stated that the County's Detention Center is now operating under the new booking system computer software. The process is going smoothly.

PUBLIC COMMENT:

The Chairwoman McGhaney asked if anyone wished to speak to Council during public comment. No one spoke during public comment.

ADJOURNMENT:

There being no further business and no additional comments from the public, the meeting was adjourned at 6:35 p.m. after a motion, a second, and unanimously carried by Council.

Respectfully submitted,

Vivian Fleming McGhaney

Chairman or Vice Chairman
Sumter County Council

Mary W. Blanding

Clerk to County Council
Sumter County Council

Approved _____

I certify that public and media notification of the above-mentioned meeting was given prior thereto as follows:

Public Notified: Yes

Manner Notified: Agendas posted on bulletin board on third floor of the Administration Building.

Date Posted: April 20, 2009

Media Notified: Yes

Manner Notified: Agendas were sent to most radio stations, television stations, and newspapers in the Sumter, Columbia, Manning, and Florence communities. Also, E-Mail notification was sent to Sumter County's Home Page, WIBZ, The Item, The Chamber, Time Warner Cable.

Date Notified: April 20, 2009

Respectfully submitted,

Mary W. Blanding
Mary W. Blanding

Sumter County, South Carolina
Identity Theft Prevention Policy

PURPOSE

The purpose of this written policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, and South Carolina Act 190 of 2008, the Financial Identity Fraud and Identity Theft Protection Act.

DEFINITIONS

Covered Account: means an account that an entity or department of Sumter County offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions for which there is a reasonably foreseeable risk to customers or to the safety and soundness of account information from identity theft, including financial, operational, compliance, reputation or litigation risks.

Financial Identity Fraud: has the same meaning as the definition in SC Code of Laws §16-13-510.

Identity Theft: means fraud committed or attempted using the identifying information of another person without authority, and includes any terms and definitions as defined in SC Code of Laws §16-13-510.

Personal Identifying Information: means personal information as defined in SC Code of Laws §16-13-510(D). It does not mean information about vehicular accidents, driving violations, and driver's status.

Security Breach: means an incident of unauthorized access to and acquisition of records or data that was not rendered unusable through encryption, redaction, or other methods containing personal identifying information that compromises the security, confidentiality, or integrity of personal identifying information maintained by a person when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the consumer.

Red Flag: means a pattern, practice or specific activity that indicates the existence of possible identity theft.

PROGRAM

Sumter County establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;
4. Eliminate risk factors that are determined to increase the risk of a security breach;
5. Minimize the instances that lawfully obtained personal identifiable information is disseminated as required pursuant to applicable portions of South Carolina Act 190 of 2008;
6. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

ADMINISTRATION

1. The Sumter County Administrator shall be responsible for the development, implementation, oversight and continued administration of the program;
2. The Program shall train staff as necessary, to effectively implement the program; and
3. The Program shall exercise appropriate and effective oversight of service provider arrangements.
4. Enclosures (1) Assessment Worksheet and (2) Addition to the Personnel Manual concerning confidentiality are attached hereto are to be used to comply with this policy.

MANAGEMENT AND SECURITY OF PERSONAL IDENTIFYING INFORMATION

The Sumter County Administrator shall enact procedures to manage and secure lawfully obtained personal identifying information maintained so that it shall only be disseminated internally for use by employees of the entity for legitimate business reasons, and externally to the general public only for reasons authorized by state, federal or local statutes;

Sumter County shall disclose a breach in the security data to a resident of this state whose unencrypted and un-redacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person, when the illegal use of the

information has occurred or is reasonably likely to occur. Disclosure shall be done in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in SC Code of Laws §1-11-490(C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

IDENTIFICATION OF RED FLAGS

1. The Program shall include relevant red flags from the following categories as appropriate:
 - a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
 - b. The presentation of suspicious documents;
 - c. The presentation of suspicious personal identifying information;
 - d. The unusual use of, or other suspicious activity related to, a covered account; and
 - e. Notice from customers, victims of identity theft, law enforcement authorities, state, federal or local government entities, or other persons regarding possible identity theft in connection with covered accounts.
2. The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:
 - a. The types of covered accounts offered and maintained;
 - b. The methods provided to open covered accounts;
 - c. The methods provided to access covered accounts; and
 - d. Its previous experience with identity theft.
3. The program shall incorporate relevant red flags from sources such as:
 - a. Incidents of identity theft previously experienced;
 - b. Methods of identity theft that reflect changes in risk; and
 - c. Applicable supervisory guidance.

DETECTION OF RED FLAGS

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information, and verifying the identity of a person opening a covered account; and
2. Authenticating individuals, monitoring transactions, and verifying the validity of change of account information requests in the case of an existing covered account.

RESPONSE

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the business arrangements of the organization.

OVERSIGHT OF THE PROGRAM

Oversight of the Program shall include:

1. Assignment of specific responsibility for implementation of the program;
2. Review of reports prepared by staff regarding compliance; and
3. Approval of material changes to the Program as necessary to address changing risks of identity theft.

Reports shall be prepared as follows:

1. Staff responsible for development, implementation and administration of the Program shall report to the Sumter County Administrator at least annually on compliance by the organization with the Program.
2. The report shall, at a minimum, address material matters related to the program and evaluate the following:
 - a. The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - b. The minimum standards that vendors must adhere to pursuant to a Service provider agreement;
 - c. Significant incidents involving identity theft and management's response; and
 - d. Recommendations for material changes to the Program.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The organization shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a

service provider to perform an activity in connection with one or more covered accounts.

DUTIES REGARDING DATA DISCREPANCIES

The organization shall develop policies and procedures designed to enable the organization to form a reasonable belief that customer data relates to the consumer for whom it was requested if the organization receives a notice of discrepancy from a nationwide consumer reporting agency indicating the data given by the consumer differs from data contained in the consumer report.

1. The organization may reasonably confirm that account data is accurate by any of the following means:
 - a. Verification of the data with the consumer;
 - b. Review of the utility's records;
 - c. Verification of the data through third-party sources; or
 - d. Other reasonable means.

2. If accurate data is confirmed, the organization shall furnish the consumer's data to the nationwide consumer reporting agency from which it received the notice of discrepancy if:
 - a. The organization establishes a continuing relationship with the consumer; and
 - b. The organization, regularly and in the ordinary business, furnishes information to the consumer reporting agency.

William T. Noonan
Sumter County Administrator

**Approved by Sumter County Council
April 28, 2009**

Enclosure 1 to
SUMTER COUNTY PRIVACY / IDENTITY THEFT POLICY

Assessment Worksheet

1.Division/Department:

2.Name/TitleofPersonAnswering:

3. What sensitive information, including personal identifying information, does your Department collect or have access to? (CHECK ALL THAT APPLY)

- * Social security numbers _____
 - * Checking account numbers _____
 - * Credit card numbers _____
 - * Personal identification numbers _____
 - * Electronic identification numbers _____
 - * Electronic passwords _____
 - * License numbers _____
 - * Telephone numbers _____
 - * Birth Certificates _____
 - * Other numbers or information which may be used to access a person's financial resources _____
 - * Driver's license numbers _____
 - * Savings account numbers _____
 - * Debit card numbers _____
 - * Digital signatures _____
 - * Employee id's _____
 - * Health information _____
 - * Immigration papers _____
- (specify)

4. For what purpose:

5. Who has access to the personal information?

Please identify by position(s):

6. Could anyone else get a hold of it? Yes _____ No _____

If "yes", who and how?

—

7. Where is the personal information kept? (CHECK ALL THAT APPLY)

* Desk-top computers _____

* Lap top computers _____

* Flash Drives _____

* Home Computers _____

* Cell phones _____

* File cabinets _____

*

Other

(specify)

8. Who inventories and maintains the records and equipment described above? (ID by Dept or position, e.g. IT, Records Retention, 3rd party vendors)

9. Who sends personal information to you? (CHECK ALL THAT APPLY)

* Inter-office _____

* Other governmental entities _____

* The individual consumer / applicant/ taxpayer/ visitor, etc. _____

* Another on behalf of an individual _____

* Private sources, e.g. banks, credit service, etc. (specify)

* _____ Other (Specify)

10. How do you receive the personal information? (CHECK ALL THAT APPLY)

* Paper _____ * Verbal (in person) _____ * Verbal (telephone) _____

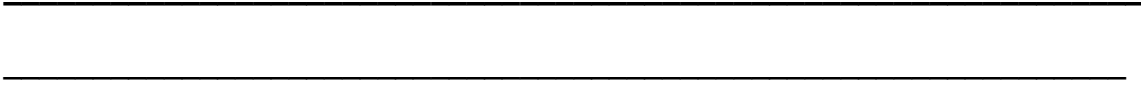
* web-site _____ * E-mail _____ * Radio _____

* _____ Other (specify)

11. Is any of the personal identifying information published, i.e. printed on any invoices or other forms that are mailed? If so, please describe.

12. When, how, and by whom is information destroyed?

13. If not destroyed, what becomes of it (e.g. Archives, microfilm, digital retention, etc.)?



Enclosure 2 to
SUMTER COUNTY PRIVACY / IDENTITY THEFT POLICY

ADDITION TO PERSONNEL POLICY

CONFIDENTIALITY

Policy:

All officers, employees, contractors, agents, and volunteers who access or have access to personally identifiable information or personally identifiable financial information will sign a Confidentiality Statement that such information will be held in confident with the understanding that any violation of the confidentiality may result in disciplinary action up to and including dismissal, dissolution of contractual agreement, and possible civil or criminal penalties.

Purpose:

1. To establish a consistent policy for all officers, employees, contractors, agents, and volunteers accessing or having access to personally identifiable information or personally identifiable financial information to sign a Confidentiality Statement.
2. To ensure confidentiality of personally identifiable information or personally identifiable financial information within Sumter County regardless of the method of storage.
3. Currently employed staff will sign the first working day of the new year and will be witnessed by their manager or their manager's designee.
4. The Confidentiality Statement will remain in the individual's personnel file or with the contract as appropriate.
5. Confidentiality training on the handling of sensitive information, including but not limited to personally identifiable financial information, will be a part of the County's orientation process and will continue on an annual basis.

Confidentiality Policy & Agreement (Internal)

All paper and electronically-stored files and records of Sumter County Government, which may or may not contain personally identifiable information or personally identifiable financial information, are the exclusive property of Sumter County government. Any unauthorized dissemination, transfer, duplication or storage of such material(s) is expressly prohibited.

I understand, and it has been fully explained to me, that maintaining confidentiality both during and subsequent to my employment with the County of Sumter, South Carolina, is of utmost importance. I am aware and have been fully informed that Sumter County routinely handles sensitive, personally identifiable information that must not be shared with any unauthorized person, unless dissemination of such information is to persons or agencies legitimately having an interest in the information, e.g. law enforcement agencies, Department of Revenue, etc., and only then in pursuance of my duties.

Any computer data, whether on hard systems, software, or removable media, including but not limited to payroll, accounts receivable, accounts payable, LEADS, NCIC, Gear, and Debt-Set-off data, and accompanying software, police, emergency services, and financial data reports, memoranda, records, case-files, investigative materials, and documents, together with verbal information will be used only for the business purposes of Sumter County government.

I am fully aware that an employment position with Sumter County Government demands a high degree of trust and that maintaining strict confidence in what occurs or is seen on the job is essential. I understand and agree that unauthorized disclosure or dissemination by me of information derived from or during my employment with Sumter County Government, either during or after my employment, will constitute the basis for disciplinary action, up to and including termination, and/or legal action.

Signed this _____ day of _____, 200____.

Employee signature

Witness:
