CITY OF GRISWOLD

General Policy/Procedure
Shredding of Sensitive Information

ADOPTION DATE: October 10, 2011

RESOLUTION NUMBER: 7-2012

REVIEW PERIOD: This policy is to be reviewed every three years or as needed.

STATEMENT OF POLICY

It is the City of Griswold's policy to ensure that all sensitive and/or personal information is handled carefully and responsibly in order to avoid being abused for improper or illegal activities. The City takes reasonable measures to protect against unauthorized access of sensitive information in connection with the disposal of documents and records.

APPLICABILITY

This policy applies to all employees of the City of Griswold that have access to, handle, store, and/or dispose of paper documents, electronic media, or other media containing sensitive information.

DEFINITIONS

Sensitive Information- information that is subject to privacy considerations or has been classified as confidential and subject to protection from public access or inappropriate disclosure. It includes, but is not limited to:

- Social Security Number, Home and mailing address, Home phone number, Date of Birth/Age, Ethnicity, etc.
- Health/Medical records including anything covered by the Health Insurance Portability and Accountability Act (HIPAA)
- Job applicant records (Names, transcripts, etc.)
- Employment and payroll records

Electronic Media- Includes any non-paper material or media on which information can be stored or preserved, including, but not limited to, computers, laptops, notebooks, tablet computers, phones, computer hard drives, zip drives, "thumb" drives, floppy disks, USB flash drives, memory sticks, magnetic tape, or other electromagnetic or electromechanical means of storing data, and includes optical storage media such as CDs or DVDs.

POLICY AND PROCEDURE

Prior to disposing of documents or electronic and other media by any non-secure method, individuals who dispose of documents or electronic and other media containing personal information must review it to ensure that it does not contain sensitive information as defined by this policy.

PAPER DOCUMENTS

All employees disposing of paper documents, microfilm, photographs, negatives, and similar media which contain sensitive information must do so by one of the following methods:

1. *Dispose of Paper Documents by Staff/Employees*
   If disposing of documents containing sensitive information through shredding or pulverizing, the responsible individual must check the document after destruction to determine whether the sensitive information can be read. If so, the document should be re-shredded, cross-shredded, or re-pulverized, and checked again. If the document cannot be shredded or pulverized so as to make its contents unreadable, the document should be set aside for burning or other destruction methods.

2. *Documents to be Destroyed by Service Provider*
   A third-party for document destruction services may be obtained. In this case, the documents are placed in secure disposal containers for disposal by the destruction service provider. The City Administrator will be responsible to ensure the third party has the means to comply with the restrictions of this policy. This normally requires a certification from the vendor and a receipt of all records destroyed. These certifications and receipts must be kept in the project/program office.

ELECTRONIC MEDIA

An employee disposing of electronic media or non-paper and non-electronic media containing sensitive information shall do so by one of the following methods:

1. *Computers, Servers, Phones, and PDA, Notebooks, Tablet Computer Devices*
   Before these devices are sold, leased, donated, recycled, or otherwise transferred to a third party for further use, the hard drive(s) shall be erased and reformatted using a software program designed to ensure the secure destruction of sensitive information or removed from the unit.

   If sensitive information cannot be securely erased from the device, the hard drive or other component containing the sensitive information shall be securely destroyed by a third party vendor certified to perform this type of physical destruction. If the devices containing sensitive information are to be disposed of, rather than transferred to a third party for further use, the hard drive(s) of the device and any recording or memory unit of the device containing sensitive information shall either be physically removed and destroyed by breaking the drive, or the drive or unit must be wiped by a suitable degaussing magnet.

2. *Storage Media (i.e. Zip Drives, Disks, Flash Drives, Optical Storage Media, etc.)*
   Prior to disposal, all electronic data storage media such as external hard drives, zip drives, tape drives, floppy disks, memory cards, memory sticks, USB flash drives, or other electronic storage media containing sensitive information shall have the data contained in the item destroyed by either wiping the media with a degaussing magnet, or by physically destroying the media through shredding or similar physical destruction. CD's, DVD's, and other optical storage media must be disposed of by physical destruction of the media, such as by shredding. Disposal may also be accomplished by providing the electronic storage media or optical storage media to a third-party destruction.

Employees should immediately notify the City Administrator or the Mayor of any violation of this policy, or of any concerns they may have regarding the secure disposal or destruction of sensitive information. Violations of this policy may result in disciplinary action up to and including termination of employment. Violators may also be subject to applicable civil and/or criminal penalties.