STOREY COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER: 024
EFFECTIVE DATE: 12-15-09
REVISED: 04/17/18 – 01/13/2020
AUTHORITY: BOC
COUNTY MANAGER: AO

SUBJECT: PRIVACY OF STOREY COUNTY IT RESOURCES

I. PURPOSE/POLICY: Storey County understands the diversity of values in a government institution and so it is respectful of freedom of expression. The county does not condone censorship, nor does it endorse the systematic inspection of electronic files or monitoring of network activities related to individual activities. However, there are legitimate reasons for persons other than the account holder to access computer files or computers or network traffic: ensuring the continued integrity, security, or effective operation of county systems; to protect user or system data; to ensure continued effective departmental operations; to ensure appropriate use of county systems; or to satisfy a lawful court order.

II. PROCEDURE: Stored computer information, voice and data network communications, email and personal computers may not be accessed by someone other than the person to whom the computer or account in which the information has been stored is assigned, or from whom the communication originated, or to whom the device has been assigned, outside of the provisions of this policy. This policy covers:

- Data and other files, including electronic mail and voice mail, stored in individual computer accounts on county-owned centrally-maintained systems;
- Data and other files, including electronic mail and voice mail, stored in individual computer accounts on systems managed by the county on behalf of affiliated organizations;
- Data and other files, including electronic mail or voice mail, stored on personally-owned devices.
- Data and other files, including electronic mail or voice mail, stored on county owned computers assigned to a specific individual for their use in support of job functions; and
- Telecommunications (voice or data) traffic from, to, or between any devices described above.

A technician or administrator may access or permit access to the resources described above, if he or she;

1. Has been directed by the department head or elected official with concurrence of IT Director to access or provide access; or
2. In an emergency situation, has a reasonable belief that a process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to system or other users' data; or

3. Receives authorization from the County Manager, Administrative Officer and/or IT Department, for situations where there is reasonable belief that the individual or a user to whom the account or device is assigned or owned has perpetrated or is involved in illegal activities using the accounts or device in question; or
4. Receives authorization from the County Manager, Administrative Officer and/or IT Department, for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has perpetrated or is involved in violations of county policy using the accounts or device in question; or
5. Receives a request from the Department Head to access the account of staff who is deceased, terminated, or is otherwise incapacitated or unavailable, for the purposes of retrieving material critical to the operation of the department; or
6. Receives a directive from the County Manager, Administrative Officer, legal counsel and/or IT Department regarding investigations of fiscal misconduct; or
7. Receives a legal court order and subsequent direction from Storey County legal counsel, or
8. Receives other legal documents and subsequent direction from Storey County legal counsel.

In the event that county officials are notified of an investigation for alleged misconduct or unauthorized activity by an employee, contents of the employee's e-mail, other computer accounts, office computer, or network traffic may be copied and stored to prevent destruction and loss of information, pending formal review of that material. Subsequent release of the stored materials must be in accordance with the above-specified criteria.

Under normal circumstances, all efforts will be made to notify the involved individual prior to accessing the computer account or device, or before observing network traffic attributed to them. Where prior notification is not appropriate or possible, the involved individual will be notified when deemed appropriate by the department head and /or Administrative Officer.

System-generated, content-neutral information ("metadata") may be used for the purposes of monitoring system and storage utilization, problem troubleshooting, security administration, technology abuse or misuse incident investigation, and in support of formal audits. This information includes operating system logs (i.e., record of actions or events related to the operation of the system or device), user login records (i.e., what usernames were used to connect to Storey County systems, from where, and when) dial-up logs (i.e., who connected to Storey County modems, from where, and when), network activity logs (i.e., what connections were attempted or completed to Storey County systems, from where, and when), email logs (i.e., who sent email to or from Storey County email systems, and when), and auditing logs (i.e., records of what actions were taken on Storey County systems, against what resources or applications, and when). The IT Department will be responsible for collecting, maintaining and protecting this data, and will forward it to the appropriate agencies if requested.

Any intrusive or restrictive actions taken by the county related to information technologies will be in accordance with guidelines and procedures set forth in other applicable county policies, codes, or laws. County policies include (but are not limited to) the administrative procedures and policies, and technology appropriate use policies. Laws include, but are not

limited to, the Health Information Portability and Accountability Act (HIPAA) (patient medical information), Electronic Communication Privacy Act, the No Electronic Theft Act, and the Digital Millennium Copyright Act. Individual Departments may have additional policies which may be more restrictive.

III. PROCEDURE REFERENCE: Where possible and feasible, technicians receiving requests for access to computer accounts, files, or network traffic by persons other than the account holder will consult with the IT Director and County Manager and/or Administrative Officer prior to granting the access. The IT Director and Administrative Officer and/or County Manager will ensure that that the provisions of this policy have been followed. Where prior consultation is not appropriate or possible, the involved individual will be notified when deemed appropriate by the IT Director, County Manager and/or Administrative Officer. It is important to note that Storey County complies with laws and standards such as HIPAA and NCJIS. Some systems such as the State NCJIS may require criminal background checks before access is granted.

Court orders and other legal documents requiring access should be delivered to the County Manager and/or District Attorney as well as the IT Director. Under any other circumstances, the document will be immediately sent to Storey County District Attorney's office. Storey County legal counsel will review the order and take appropriate action.

IV. RESPONSIBILITY FOR REVIEW: This policy will be reviewed on an annual basis or as needed by the Information Technology Director and Administrative Officer or HR Director.