STOREY COUNTY ADMINISTRATIVE POLICIES AND PROCEDURES

NUMBER:	**027**
EFFECTIVE DATE:	**12/15/09**
LAST REVISED:	**06/04/24**
AUTHORITY:	**BOC**
COUNTY MANAGER:	**AO**

SUBJECT: IT REPORTING, SUSPENSIONS, AND INVESTIGATIONS

I. PURPOSE: This policy contains the standards and definitions for reporting abuse, outlines suspension of computer access, and describes in what manner and for what reasons investigations of alleged misconduct may be conducted.

II. APPLICABILITY: This policy applies to all Storey County staff, including elected officials, department heads, employee supervisors, administrators, and computer and network technicians, or any other authorized user.

III. PROCEDURES:

Reporting: Reports of apparent misuse or abuse of Storey County Information Technology (IT) resources are to be made to the following offices and/or authorities:

A. If the report is made by an employee, the employee shall follow the employee's immediate chain-of-command and report to the immediate supervisor.

B. The supervisor, if different from the department head shall immediately report the incident to the department head. The department head shall review the alleged violation and should consider consulting with the IT Department for assistance. If a violation is confirmed and the individual department does not have its own specific policies for disciplinary actions, it shall then be forwarded to the:

1. County Manager
2. Human Resources Director
3. IT Department

Suspension or termination of access: Department heads or IT staff may temporarily suspend or block access to an account when it appears necessary to protect the integrity, security, and functionality of county or other computing resources, or to protect the county from liability.

Access to county technology resources may be removed immediately given a request from the appropriate county authorities including, the department head, County Manager, and/or IT staff. Reasons for immediate removal may include, but are not limited to, the following: the individual is terminated for cause and there is concern for safety of systems or data; or there is reasonable belief that the individual to whom the account is assigned has perpetrated or is involved in illegal activities or activities that violate county policy.

The technician responsible for a particular service may disable access unilaterally if processes in an assigned account are causing or reasonably appear likely to cause damage to systems or data, breach data security, or may cause serious service degradation for other users. Except when prohibited by law, inappropriate, or impractical, the technician will notify the involved individual prior to disabling the computer account whenever possible. Where prior notification is not permitted, appropriate, or practical, the technician will make all efforts to notify the involved individual afterward in a timely manner. Unless other policies are invoked, access will be restored as soon as possible after the removal of the threat. In all cases the department head, Human Resources Director, and the County Manager shall be notified prior to taking such action, unless it is violating a law or causing immediate damage to any type of electronic system.

Technical Investigation: The County Manager and/or IT Department will coordinate technical investigation and computer forensics for complaints of misuse or abuse of county information technology resources. The County Manager and/or IT Department will conduct the necessary investigation and data gathering. All investigations will comply with applicable law as well as county policies and procedures.

Disciplinary Process: Reports of misuse or abuse will be resolved through established county disciplinary policies and procedures applicable to the relevant user. The county may also refer suspected violations of applicable law on the part of any individual to appropriate law enforcement agencies. Storey County Sheriff's Office, Storey County legal counsel, and law enforcement officials as appropriate shall address criminal misuse or abuse of Storey County resources by persons not affiliated with the county.

Determination of relation to purpose: If the relationship of a use of information technology resources to the county's purpose is unclear, the County Manager will coordinate with the department head involved. The County Manager, Human Resources Director, and the IT Director will collaborate to appropriately determine whether the activity is an appropriate use of county information technology resources.

Determination of incidental personal use: Department heads are authorized to define the acceptable level and nature of incidental personal use by members of the department and/or office. An employee's supervisor may require the employee to cease or limit any incidental personal use that hampers job performance or violates county policy. County technology service providers will always place a higher priority on support of county-related activities over any form of incidental personal use.

Consultation: The Human Resources and IT Departments will be available to provide consultation or advice related to technology use or misuse to any county office, department, or individual. If there are specific department exceptions they must be clearly written, approved by the County Manager and/or Human Resources Director, and clearly posted.

Identifying excessive use: The IT Director is responsible, along with the department heads, for establishing metrics for gauging excessive use.

Controls to limit excessive use may include but are not limited to established per-user limits for the service that allow for shared use of limited resources, limitations on the types of processes that can be run on a service or resource, or identification of certain uses as adversely affecting the activities of others, or adversely affecting system availability or performance. In instances where availability of a resource is constrained and where resource augmentation is not feasible or possible, the department head in consultation with the user of the resource may place limits or remove resources to protect and allow for shared use of the information technology infrastructure.

Notification of excessive use: The IT Director, and the department head of the affected information technology resource will notify the user that the user is consuming an excessive share of the resource. Upon request, users will be provided information from which they can compare their use with normal usage patterns. The IT Director or an employee of the IT Department can help identify excessive use and will work with individuals who need clarification on what may considered personal information compared to county information, as well as give operational tips for optimizing computer workstations.

Mission-related activities: If the IT Director determines that the excessive use serves the mission of Storey County, the IT Director should attempt to accommodate the needs. Accommodation may involve augmenting resources or identifying adequate alternate arrangements for fulfilling the requirements in order to find a solution that does not adversely affect other users. The user may find it necessary to cease the activity, reduce the activity to an appropriate level, or find other options.

Non-mission-related activities: If the IT Director determines that the excessive use does not serve the mission of Storey County, the user will be notified in writing to cease the activity with a copy of the notice sent to the department head and/or the County Manager.

Emergency actions: The department head, County Manager, Human Resources Director, or the IT Director may temporarily suspend or block access to an information technology resource, or stop active processes in an account, when it appears necessary to protect the integrity, security, or functionality of the resource, or to protect other computing resources, or to protect the county from potential liability.

Repeated notifications: Users who are repeatedly notified of excessive use may be subject to disciplinary measures.

IV. RESPONSIBILITY FOR REVIEW: This policy will be reviewed every five years by the IT Director.