Information & Communications Technology

COUNTY OF TULARE
AGENDA ITEM

AGENDA DATE: January 24, 2017

Public Hearing Required	Yes ☐	N/A ☒
Scheduled Public Hearing w/Clerk	Yes ☐	N/A ☒
Published Notice Required	Yes ☐	N/A ☒
Advertised Published Notice	Yes ☐	N/A ☒
Meet & Confer Required	Yes ☐	N/A ☒
Electronic file(s) has been sent	Yes ☒	N/A ☐
Budget Transfer (Aud 308) attached	Yes ☐	N/A ☒
Personnel Resolution attached	Yes ☐	N/A ☒
Agreements are attached and signature line for Chairman is marked with tab(s)/flag(s)	Yes ☐	N/A ☒

CONTACT PERSON: Jacob Kaminsky PHONE: 559-622-7308

SUBJECT: Adopt the Theft Policy and the Mobile Device Policy.

REQUEST(S):

That the Board of Supervisors:

1. Adopt the Theft Policy (Section 22) of the Information Technology Security Program.
2. Adopt the Mobile Device Policy (Section 23) of the Information Technology Security Program.
3. Adopt the changes to the Table of Contents of the Information Technology Security Program.

SUMMARY:

In 2010, this Board approved the Information Technology Security Program policies. Developed by the County's Information Technology Advisory Committee (ITAC), the purpose of this program is to define general information security responsibilities for every user of County computing assets, and to establish a documentation structure for the appropriate access to, and integrity of, County computing assets.

The proposed Theft Policy (Section 22) addresses the procedures for reasonably preventing the theft of electronic County assets, as well as outlining the protocol in the event that theft takes place or is suspected of taking place. This policy designates the persons responsible for responding to instances of theft and defines the responsibilities of all County departments for ensuring compliance with this policy.

The proposed Mobile Device Policy (Section 23) outlines the procedures for appropriate and responsible use of County-owned mobile electronic devices. This policy covers specific protocols to ensure the protection of County data and of the devices themselves.

The Information Technology Security Program serves as the minimum standard to which all County departments must adhere. Individual departments may implement additional written information security policies to meet their business needs as long as the departmental policies are consistent at all times with the overall County policies. These policies cannot be overridden or altered by any informal practice of an agency or department or by statements of supervisors or managers within a department.

FISCAL IMPACT/FINANCING:

Considering and accepting this matter will not cause a Net County Cost.

LINKAGE TO THE COUNTY OF TULARE STRATEGIC BUSINESS PLAN:

The County's five-year strategic plan includes the Safety and Security Initiative to protect businesses and individuals from white-collar crime. The plan also includes the Organizational Performance Initiative to continuously improve organizational effectiveness and fiscal stability.

ADMINISTRATIVE SIGN-OFF:

_____

William G. Harrison
Information & Communications Technology Assistant Director

cc: Auditor-Controller
County Counsel
County Administrative Office (2)

Attachment(s)
Attachment A – Table of Contents
Attachment B – Theft Policy (Section 22)
Attachment C – Mobile Device Policy (Section 23)

BEFORE THE BOARD OF SUPERVISORS
COUNTY OF TULARE, STATE OF CALIFORNIA

IN THE MATTER OF ADOPT THE THEFT POLICY AND THE MOBILE DEVICE POLICY) **Resolution No. _____**) **Agreement No. _____**

UPON MOTION OF SUPERVISOR _____, SECONDED BY SUPERVISOR _____, THE FOLLOWING WAS ADOPTED BY THE BOARD OF SUPERVISORS, AT AN OFFICIAL MEETING HELD _____ _____, BY THE FOLLOWING VOTE:

AYES:
NOES:
ABSTAIN:
ABSENT:

ATTEST: MICHAEL C. SPATA
COUNTY ADMINISTRATIVE OFFICER/
CLERK, BOARD OF SUPERVISORS

BY: _____
Deputy Clerk

* * * * * * * * * * * * * * * * * * *

1. Adopted the Theft Policy (Section 22) of the Information Technology Security Program.
2. Adopted the Mobile Device Policy (Section 23) of the Information Technology Security Program.
3. Adopted the changes to the Table of Contents of the Information Technology Security Program.

County of Tulare

Information Technology Security Program

April 6, 2010

County-Wide Information Technology Security Policies

Table of Contents

22. Theft Policy

Effective Date:
Prepared By: Information Technology Advisory Committee (ITAC)
Review Date:
Approved By: Information Technology Advisory Committee (ITAC)
Approval Date:

22.1. PURPOSE

This policy will provide guidelines for detecting and preventing theft involving County-owned equipment, assign responsibility for who detects and prevents such theft, and establish how to report known or suspected theft involving County-owned equipment.

22.2. SCOPE

This policy applies to all County-owned information systems used by employees and visitors. This includes, but is not limited to:

a. PC's, servers, network devices, printers, monitors, data center equipment, USB flash drives, Access Cards, tablets or any other device or tool that can be used to access the County network or data.

b. County-owned software regardless of location or use.

22.3. BACKGROUND

All Departments have a responsibility to efficiently conserve, preserve and employ all County resources. In accordance with County of Tulare Information Technology Security Policy 21, all County employees are responsible for safeguarding all information under their care. To this end, the County requires that appropriate security and access control systems are in place to protect County-owned equipment.

22.4. PROCEDURES

22.4.1. Prevention and Detection of Theft

22.4.1.1. Each Department is responsible for establishing the controls to prevent theft of any hardware and software assigned to their Department. Departments are required to make their employees aware of the regulations and expectations for use of County-owned equipment.

22.4.1.2. County-owned equipment will be assigned to individual County staff and will be used exclusively by that staff unless permission is expressly granted by that employee's supervisor. Equipment is to be used for the purposes of performing County business and duties as outlined by

the County of Tulare Information Technology Security Policy 2.0. and by the employee's supervisor. All equipment must be returned in proper working order in the event that an employee transitions from County employment or transfers to another Department within the County.

22.4.1.3. All County employees are responsible for the protection of County-owned assets. County employees are responsible for exercising reasonable effort to prevent any theft or damage that might occur to County-owned equipment.

22.4.1.3.1. Users must report the damage, loss or theft involving County-owned equipment to their supervisor immediately.

22.4.1.3.2. Departments will inform TCiCT of any loss, damage or theft of County-owned hardware or software as soon as possible.

22.4.1.4. Departments will ensure proper disposal of County-owned equipment based upon County Auditor and Purchasing Department Policies.

22.4.2. Burglary or Theft

If there is evidence that a burglary or theft involving County-owned hardware or software has occurred, these additional requirements apply:

22.4.2.1. Notify the appropriate law enforcement agency (Sheriff or city police) and file an incident report.

22.4.2.2. Notify the TCiCT Service Desk via a phone call or an email.

22.4.3. Investigation of Reports of Known or Suspected Theft

22.4.3.1. The Department Director shall assign an employee to investigate allegations of theft involving County-owned equipment as per established policies and procedures.

22.4.3.2. The Department Director shall be responsible for determining the extent of the loss and for reviewing and evaluating control and/or process failures related to the loss.

22.4.4. Investigation of Breach of Confidential Information

TCiCT shall conduct an investigation of a potential breach of confidential information in accordance with County of Tulare Information Technology Security Policy 21.

22.4.4.1. Reports and investigations of allegations of theft will be kept confidential to the reasonable extent possible under law and consistent with the need to conduct an adequate investigation and take corrective action.

22.5. POLICY

If appropriate County administrators conclude that an employee has engaged in theft involving County-owned hardware or software, appropriate disciplinary action will be taken, up to and including termination of employment, in accordance with applicable personnel policies.

22.6. REVISION HISTORY

Version	Date	Chapter/Section	Details

23. Mobile Device Policy

Effective Date:
Prepared By: Information Technology Advisory Committee (ITAC)
Review Date:
Approved By: Information Technology Advisory Committee (ITAC)
Approval Date:

23.1. PURPOSE

23.1.1. The purpose of this policy is to define acceptable standards for the approval, management and use of mobile devices that directly access Tulare County data. This policy does not authorize access to applications or functions that are restricted due to regulatory compliance protocols. This policy does not address accessing information made available through Tulare County public websites or social media.

23.1.2. In the event that a particular circumstance is not addressed by this policy, the user is to default to the highest possible security of client and County data. No action is to be approved or supported that threatens the security of data that is otherwise protected by County business or regulatory requirements.

23.2. SCOPE

This policy covers all mobile devices used by County employees for the purposes of official County business and procedures. Mobile devices are herein defined as any device capable of performing computing but not physically connected to the Tulare County network. These mobile devices support multiple wireless network connectivity options (primarily cellular and Wi-Fi), as well as voice and data applications.

23.3. POLICY

It is the responsibility of any Tulare County employee who utilizes a mobile device for the purposes of accessing County resources to ensure that all end user security protocols required by the Tulare County Information Security Program are also applied here. It is imperative that any mobile device that is used to conduct Tulare County business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's mobile accounts by TCiCT. Additional restrictions and/or disciplinary action may be pursued by the employee's Department Director.

23.4. PROCEDURES

All procedures are mandatory for all County employees. Failure to comply with this policy and the procedures herein will result in disciplinary action at the discretion of a non-compliant employee's supervisor and/or Department Head.

23.4.1. Access Control

23.4.1.1. TCiCT (Tulare County Information & Communications Technology) reserves the right to sever, by physical and non-physical means, a user's ability to connect mobile devices to County and County-connected infrastructure. TCiCT will engage in such action if it feels such equipment is being used in such a way that puts the County's systems or data at risk.

23.4.1.2. Prior to initial use on the County network or within related infrastructure, all County-owned mobile devices must be registered with TCiCT. TCiCT will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not connect to County infrastructure.

23.4.1.3. End users who wish to connect such devices to non-county network infrastructure to gain access to county data must employ, for their devices and related infrastructure, security measures deemed necessary by TCiCT. These may include updated software, specified anti-virus software, and personal firewalls. County data is not to be accessed on any hardware that fails to meet County-established TCiCT security standards. All mobile devices attempting to connect to the County network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by TCiCT. Devices that have not been previously approved by TCiCT, are not in compliance with TCiCT security policies, or represent any threat to the County network or data will not be allowed to connect.

23.4.2. Security

23.4.2.1. Employees using mobile devices and related software for network and data access will enroll in the county's Mobile Device Management system.

23.4.2.2. All mobile devices must be protected by a strong password. See TCiCT Security Password Policy 10 for additional details. Employees agree to never disclose their passwords to anyone.

23.4.2.2.1. Unless otherwise directed by the Department Head or required by business needs, the idle timeout must be set to a maximum of five minutes.

23.4.2.2.2. Unless otherwise directed by the Department Head or required by business needs, the grace period must be set to a maximum of one minute.

23.4.2.3. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices

used for this activity whether or not they are actually in use and/or being carried. End users are expected to adhere to County of Tulare Information Technology Security Policy 22 when in possession of County-owned mobile devices.

23.4.2.4. In the event of a lost or stolen mobile device, the user must report the loss to TCiCT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than TCiCT. If the device is recovered, it can be submitted to TCiCT for re- provisioning.

23.4.2.5. TCiCT will manage security policies, network, application, and data access centrally by using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with TCiCT security policy standards.

23.4.2.6. Employees, contractors and extra help staff will follow all TCiCT-sanctioned data removal procedures to permanently erase Tulare County - specific data from such devices once their use is no longer required.

23.4.2.7. Employees, contractors and extra help staff will make no modifications of any kind to Tulare County-owned and installed hardware or software without TCiCT's approval. Additional Department-owned applications can be purchased in accordance with section 4.6. of this policy.

23.4.2.8. TCiCT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the Tulare County network.

23.4.2.9. All mobile devices must be secured and managed by TCiCT-approved methods. Security methods will allow security policy configuration and device compliance with TCiCT monitoring and management standards and policies.

23.4.3. Mobile Device Approvals

Department Directors or designated Supervisors must provide written approval for any Tulare County employee to access County data with any mobile device. These approved users and their mobile devices are subject to all security policies and data management restrictions of their departments and TCiCT.

23.4.4. Encryption

23.4.4.1. Full device encryption and/or application-based encryption are acceptable.

23.4.4.2. On-device data at rest encryption may be hardware- or software-based

23.4.4.3. A mobile device must have data-in-motion encryption through VPN (either SSL or IPsec) or Wi-Fi (EAP TLS/WPA/WPA2).

23.4.4.4. All devices must support certificates for registration, authentication, and data encryption.

23.4.4.5. Encryption will be AES-256 or stronger.

23.4.5. Application Security

23.4.5.1. Peer-to-Peer file-sharing applications will not be used on mobile devices to access County data.

23.4.5.2. County data may only be presented or stored on TCiCT-sanctioned mobile applications.

23.4.5.3. County business can only be shared on sanctioned applications for email and other Services. Use of third party applications or services will be reviewed by the TCiCT Security Team.

23.4.6. Application Purchasing

23.4.6.1. Applications purchased for County-owned devices will be made using an account that is associated with a county email address. Any such applications purchased on a County-owned device become County property as well.

23.4.6.2. Applications may be purchased and distributed only through approved and designated department channels.

23.4.6.3. Mobile devices will be blocked from County resources when a mobile device that accesses County data is loaded with an application that is deemed a security risk, or that contains known malware.

23.4.7. Location tracking:

Location tracking may be enabled for County-owned devices. The County can remotely audit any County-managed device for County business needs. The audits may include location tracking.

23.5. REVISION HISTORY

Version	Date	Chapter/Section	Details