CONTRA COSTA COUNTY

AGENDA

Internal Operations Committee

Supervisor Diane Burgis, Chair
Supervisor Candace Andersen, Vice Chair

https://cccounty-us.zoom.us/j/85280600959
Call In: 888-278-0254 Conference code: 845965

Monday, July 8, 2024 **11:00 AM** **309 Diablo Rd, Danville**
3361 Walnut Blvd, Suite 140, Brentwood
https://cccounty-us.zoom.us/j/85280600959
Call In: 888-278-0254 Conference code: 845965

Agenda Items: Items may be taken out of order based on the business of the day and preference of the Committee.

1. Call to Order

2. Public comment on any item under the jurisdiction of the Committee and not on this agenda (speakers may be limited to two (2) minutes).

3. RECEIVE and CONSIDER approving the Record of Action for the June 10, 2024 Internal Operations Committee meeting. (Jason Chan, County Administrator's Office) **24-1978**

Attachments: DRAFT IOC ROA 6-10-24

4. RECEIVE presentation on the proposed Information Security Policy and CONSIDER approving the recommended policy for Board of Supervisors consideration or providing direction to staff on any changes. (Marc Shorr, Chief Information Officer) **24-1979**

Attachments: Presentation: Admin Bulletin on Information Security
Final Draft: Information Security Administrative Bulletin
Sample Electronic Data Management Plan

The August 12, 2024 meeting has been canceled. The next meeting is currently scheduled for September 9, 2024.

Adjourn

General Information

This meeting provides reasonable accommodations for persons with disabilities planning to attend a the meetings. Contact the staff person listed below at least 72 hours before the meeting. Any disclosable public records related to an open session item on a regular meeting agenda and distributed by the County to a majority of members of the Committee less than 96 hours prior to that meeting are available for public inspection at 1025 Escobar St., 4th Floor, Martinez, during normal business hours. Staff reports related to items on the agenda are also accessible on line at www.co.contra-costa.ca.us.

HOW TO PROVIDE PUBLIC COMMENT:
Persons who wish to address the Committee during public comment on matters within the jurisdiction of the Committee that are not on the agenda, or who wish to comment with respect to an item on the agenda, may comment in person, via Zoom, or via call-in. Those participating in person should offer comments when invited by the Committee Chair. Those participating via Zoom should indicate they wish to speak by using the "raise your hand" feature in the Zoom app. Those calling in should indicate they wish to speak by pushing *9 on their phones.

Public comments generally will be limited to two (2) minutes per speaker. In the interest of facilitating the business of the Board Committee, the total amount of time that a member of the public may use in addressing the Board Committee on all agenda items is 10 minutes. Your patience is appreciated.

Public comments may also be submitted to Committee staff before the meeting by email or by voicemail. Comments submitted by email or voicemail will be included in the record of the meeting but will not be read or played aloud during the meeting.

For Additional Information Contact: Jason Chan, Sr. Deputy County Administrator; jason.chan@cao.cccounty.us

1025 ESCOBAR STREET
MARTINEZ, CA 94553

CONTRA COSTA COUNTY

Staff Report

File #: 24-1978 **Agenda Date:** 7/8/2024 **Agenda #:** 3.

INTERNAL OPERATIONS COMMITTEE
Meeting Date: July 8, 2024
Subject: Record of Action for the June 10, 2024 IOC Meeting
Submitted For: Monica Nino
Department: County Administrator
Referral No:
Referral Name:
Presenter: Jason Chan
Contact: Julie.enea@cao.cccounty.us

Referral History:
County Ordinance requires that each County body keep a record of its meetings. Though the record need not be verbatim, it must accurately reflect the agenda and the decisions made in the meeting.

Referral Update:
Attached is the Record of Action for the June 10, 2024 Internal Operations Committee meeting.

Recommendation(s)/Next Step(s):
RECEIVE and APPROVE the Record of Action for the June 10, 2024 Internal Operations Committee meeting

Fiscal Impact (if any):
None.

CONTRA COSTA COUNTY

Committee Meeting Minutes

Internal Operations Committee

Supervisor Diane Burgis, Chair
Supervisor Candace Andersen, Vice Chair

https://cccounty-us.zoom.us/j/85280600959
Call In: 888-278-0254 Conference code: 845965

Monday, June 10, 2024 **11:00 AM** **1516 Kamole Street. Honolulu, HI | 3361 Walnut Blvd, Suite 140,Brentwood | https://cccounty-us.zoom.us/j/85280600959 | Call In: 888-278-0254 Conference code: 845965**

1. Call to Order

Chair Burgis called the meeting to order at 11:01 a.m. In addition to the Committee members, the following individuals were in attendance: Eric Angstadt, Steve Kowalewski, Jill Ray, Alicia Nuchols, Tavane Payne, Jennifer Bruggeman, Jeffrey Acuff, and Julie Enea.

Present: Diane Burgis and Candace Andersen

2. Public comment on any item under the jurisdiction of the Committee and not on this agenda (speakers may be limited to two (2) minutes).

No one requested to speak during the general public comment period.

3. RECEIVE and APPROVE the Record of Action for the May 13, 2024 Internal Operations Committee meeting. (Julie Enea, County Administrator's Office)

Attachments: DRAFT IOC ROA 5-13-24

Approved as presented.

Aye: **Chair Burgis and Vice Chair Andersen**
Result: **Passed**

4. ACCEPT report from the County Administrator on process undertaken to update Administrative Bulletin No. 527, "Capital Projects and Real Estate Services" and CONSIDER approving the updated Bulletin and directing the County Administrator to prepare all necessary actions to implement the policy for consideration by the full Board of Supervisors, or PROVIDE any additional direction to staff as needed. (Eric Angstadt, County Administrator's Office)

Attachments: ATTACHMENT A - Referral to IOC - 2023 Admin Bulletins 4-24-
ATTACHMENT B - Admin Bulletin 527 Capital Projects and Real Estate Services_final draft

Chief Asst. County Administrator Eric Angstadt presented the staff report, proposed policy, and recommendations.

Vice Chair Andersen asked if this policy would help avoid past issues experienced with some Health Services Department facilities projects, to which Eric responded that it would and that he was currently developing an RFP for the care court and inpatient treatment facility projects. He also confirmed that Public Works Director Warren Lai and several others assisted with development of the policy.

Eric reported that for FY 24/25, 20 of 40 requested capital projects were approved to proceed. He noted the two levels of CAO review: capital planning (himself) and finance (Adam Nguyen). Projects were considered and prioritized in terms of need, urgency, cost and funding source, timing, and capacity to manage/implement the jobs. Some projects were moved up in priority if there was ability to bundle them with similar projects to achieve economies of scale. He also stated that Capital Projects' staff capacity had been increased in anticipation of the new policy and procedures, which attempt to funnel project requests through the annual budget process. He also reported that more robust project management software will be implemented to better support the entire process.

The Committee unanimously approved the proposed Capital Facilities Policy and directed staff to forward it to the Board on Consent.

Aye: **Chair Burgis and Vice Chair Andersen**

Result: **Passed**

5. CONSIDER the Mental Health Commission's proposed changes to its bylaws pertaining to attendance. (Julie Enea or Laura Griffin, Commission Chair)

Attachments:
MHC Bylaws Last Updated Sept 2021
Mark-up of Proposed Changes from Sept 2021 version - Attendance Section Only
Final Draft of Changes from Sept 2021 version - Attendance Section Only

Julie Enea provided background for the recommendation. Vice Chair Andersen advised that Proposition 1 will necessitate combining the Alcohol and Other Drugs Advisory Board with the Mental Health Commission (MHC) (or decommissioning those bodies and creating a new body), and that the Family and Human Services Committee would likely be working on that effort. Still, the IOC agreed that the proposed MHC bylaw amendments could move forward in the interim.

Jennifer Bruggeman advised that the MHC requires 8 attendees to achieve a Commission quorum, which is usually achieved. However, she said that MHC subcommittees have had more difficulty achieving a quorum due to their small size.

Vice Chair Andersen said the proposed amendments were important because they define what constitutes an excused absence and provides a procedure to report and recognize excused absences. This is especially important for Commissioners who have professional obligations, particularly involving travel, that prevents attendance at MHC meetings.

Tavane Payne urged the IOC to approve the amendments even if they will only be

operational for the remainder of the calendar year.

The IOC approved the proposed bylaw changes and directed staff to forward them to the Board on Consent.

Aye: **Chair Burgis and Vice Chair Andersen**

Result: **Passed**

6. The next meeting is currently scheduled for July 8, 2024.

Staff advised that CAO Senior Deputy Jason Chan would provide Committee staff support at the July 8 meeting.

7. Adjourn

Chair Burgis adjourned the meeting at 11:29 a.m.

General Information

This meeting provides reasonable accommodations for persons with disabilities planning to attend a the meetings. Contact the staff person listed below at least 72 hours before the meeting. Any disclosable public records related to an open session item on a regular meeting agenda and distributed by the County to a majority of members of the Committee less than 96 hours prior to that meeting are available for public inspection at 1025 Escobar St., 4th Floor, Martinez, during normal business hours. Staff reports related to items on the agenda are also accessible on line at www.co.contra-costa.ca.us.

HOW TO PROVIDE PUBLIC COMMENT:
Persons who wish to address the Committee during public comment on matters within the jurisdiction of the Committee that are not on the agenda, or who wish to comment with respect to an item on the agenda, may comment in person, via Zoom, or via call-in. Those participating in person should offer comments when invited by the Committee Chair. Those participating via Zoom should indicate they wish to speak by using the "raise your hand" feature in the Zoom app. Those calling in should indicate they wish to speak by pushing *9 on their phones.

Public comments generally will be limited to two (2) minutes per speaker. In the interest of facilitating the business of the Board Committee, the total amount of time that a member of the public may use in addressing the Board Committee on all agenda items is 10 minutes. Your patience is appreciated.

Public comments may also be submitted to Committee staff before the meeting by email or by voicemail. Comments submitted by email or voicemail will be included in the record of the meeting but will not be read or played aloud during the meeting.

For Additional Information Contact:

File #: 24-1979 **Agenda Date:** 7/8/2024 **Agenda #:** 4.

INTERNAL OPERATIONS COMMITTEE
Meeting Date: July 8, 2024
Subject: County Information (Cyber) Security Policy
Submitted For: Monica Nino
Department: County Administrator
Referral No: IOC 24/8
Referral Name: Update of County Administrative Bulletins/Policies
Presenter: Marc Shorr, Chief Information Officer, Department of Information Technology
Contact: Marc Shorr, marc.shorr@doit.cccounty.us

Referral History:
On April 24, 2023, the Board referred to the IOC a review of several existing administrative policies:

1. Administrative Bulletin No. 525, "Office Space"
2. Administrative Bulletin No. 525.1, "Requesting Real Estate and Capital Project Services"
3. Administrative Bulletin No. 526, "Real Estate Asset Management Policy"
4. Administrative Bulletin No. 600, "Purchasing Policy and Procedures";

And, creation of the following new Administrative Bulletins:

1. Social Media Policy (Updating and replacing 2014 policy)
2. Cybersecurity Policy (New policy).

On June 27, the IOC recommended, and the Board approved, updated Purchasing policies and procedures. On July 11, the IOC recommended, and the Board adopted, an Ordinance amending the Purchasing Agent's authority to execute contracts for special services under Government Code section 31000 by eliminating the requirement that these contracts be first reviewed, approved, and signed by the County Administrator.

On August 1, the IOC recommended, and the Board approved with amendments, updates to the County's Social Media Policy, which prompted a new referral to the IOC regarding institution of a countywide ban on the TikTok social media application. The proposed TikTok ban has been suspended pending the outcome of a First Amendment challenge filed in May in the U.S. Court of Appeals for Washington, D.C.

As the County Administrator completes other policy updates, the final drafts are brought to the IOC for review and input.

Referral Update:
Today, the IOC is asked to review and provide direction on the final draft of the Information Security Policy, attached. The policy outlines the responsibilities of County departments to inventory their data and IT equipment, design and implement security measures to protect County data and IT systems, respond promptly to cybersecurity events by reporting them to Department of Information Technology (DoIT) and initiating data

recovery protocols, and ensure that staff receive appropriate and relevant training. The policy also outlines DoIT's responsibilities to assist County departments in maintaining information security, install cybersecurity defenses and monitor their effectiveness, and help detect, investigate, and recover from cybersecurity events. The County Administrator will be responsible for overseeing policy compliance.

Chief Information Officer Marc Shorr and DoIT staff will present the proposed policy and be available to respond to any questions or comments the committee may have.

Recommendation(s)/Next Step(s):
RECEIVE presentation on the proposed Information Security Policy and CONSIDER approving the recommended policy for Board of Supervisors consideration or providing direction to staff on any changes.

Fiscal Impact (if any):
None.

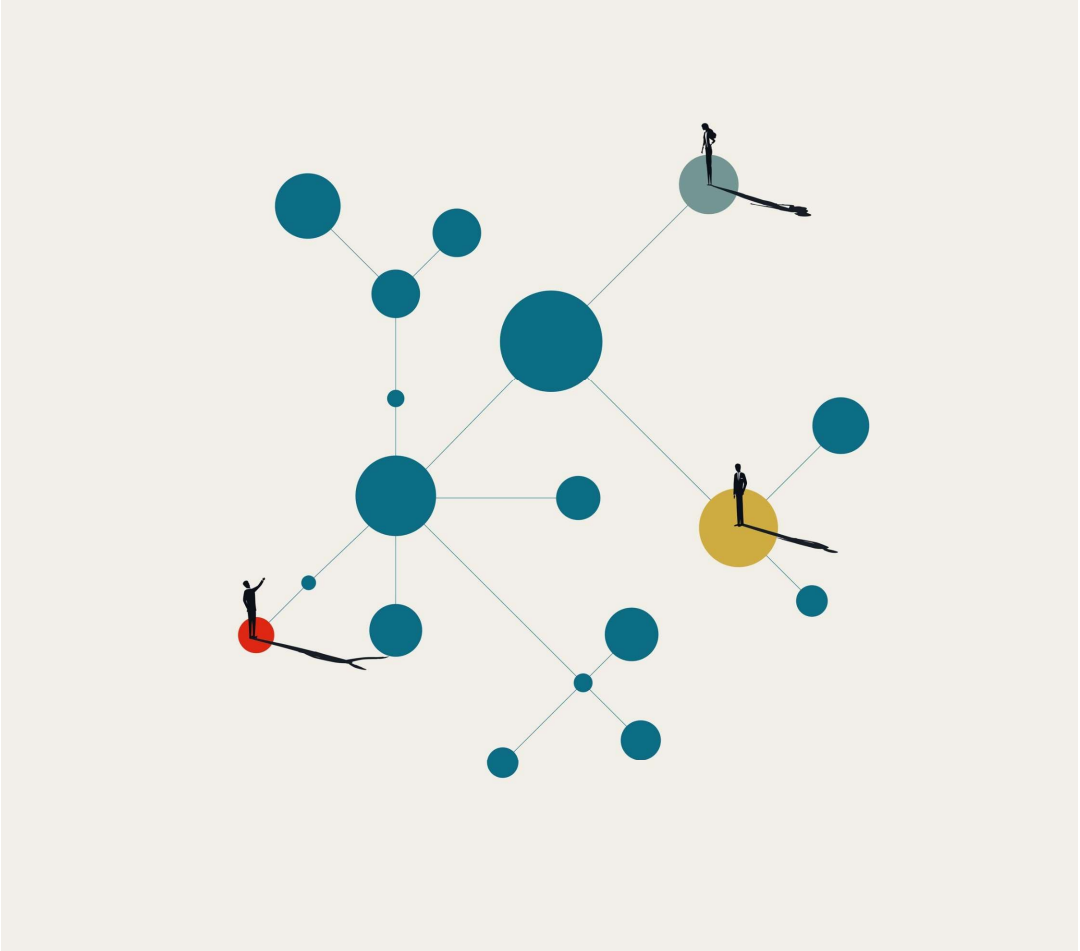
Information Security Administrative Bulletin

DEPARTMENT OF INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

Why Are We Here

In today’s world, the security landscape is characterized by increasingly sophisticated and frequent cyber threats. Local governments, including ours, struggle to handle these threats due to resource constraints and fragmented approaches.

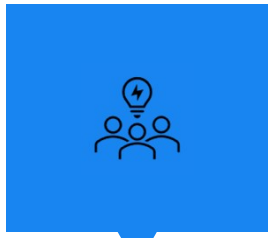


DEPARTMENT OF INFORMATION TECHNOLOGY

How We Got Here

Developed in alignment with the County's cybersecurity strategy, this initiative was a collaborative process involving multiple County departments. The document was edited and reviewed by County Counsel’s Office.

This Bulletin will establish a solid foundation, equipping the organization to effectively confront both current and future cybersecurity threats.



Establishes a framework for implementing consistent safeguards across all the organization.

Governance

Our governance approach includes socializing proposed standards and weighing business impact prior to adoption. This collaborative process ensures we understand the impact security safeguards will have on County service delivery.

DEPARTMENT OF INFORMATION TECHNOLOGY

Security Awareness Training

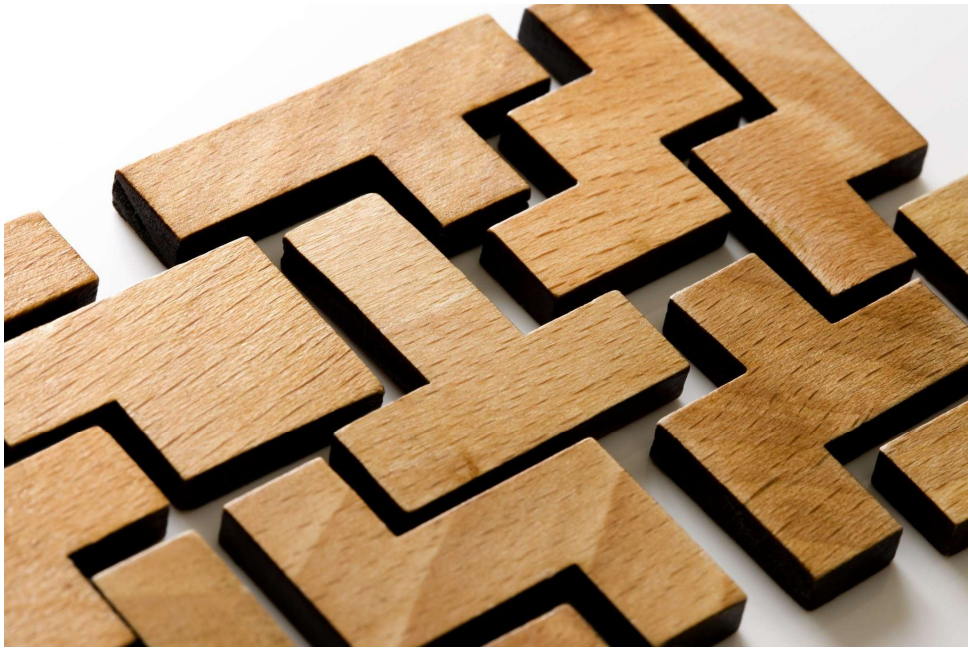
According to the FBI's Internet Crime Complaint Center statistics the most common category of reported cyber crime involves a human element, such as email phishing or vendor impersonation attacks.

Our people are our first and most crucial line of defense. It is essential we prepare our County staff with training to identify and prevent cybersecurity incidents. While most County staff already receive some form of security awareness training, this policy will ensure consistent training across the County.

DEPARTMENT OF INFORMATION TECHNOLOGY

What's Next?

This Administrative Bulletin establishes a robust foundation for the County to operate information technology systems and securely deliver services to our community in a collaborative fashion.

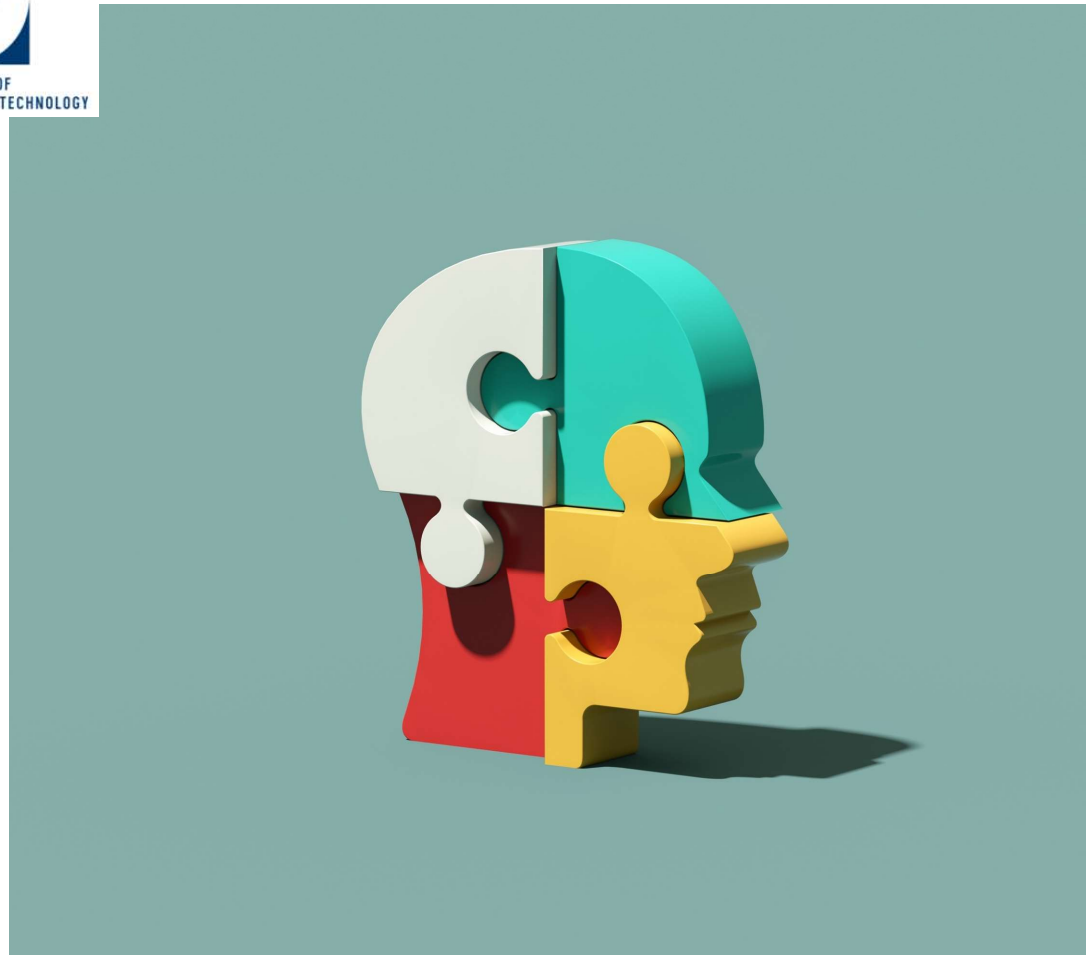


DEPARTMENT OF INFORMATION TECHNOLOGY

DoIT Recommendations

1. Request Committee approve bulletin
2. Request County Administrator bring bulletin forward for Board of Supervisors approval

DEPARTMENT OF INFORMATION TECHNOLOGY



Thank You!

Questions from the committee?

I. **PURPOSE.** Cyberattacks are digital attacks that are usually aimed at accessing, changing or destroying sensitive electronic information; extorting money from electronic device users via ransomware; or interrupting normal business operations. Common types of cyberattacks include denials of service, phishing, and ransomware attacks. As cyberattacks continue to increase, it is important for the County to implement a countywide framework to prevent disruption to operations and to avoid data breaches.

Preventing and minimizing the effects of cyberattacks requires electronic data management, electronic security measures and a cyberattack response plan. This bulletin provides standards for County departments in these areas. And because all employees are key in maintaining cybersecurity, this bulletin also recognizes the importance of training employees about their role in protecting the County's electronic systems and data.

II. **AUTHORITY.** In accordance with County Ordinance Code Section 24-4.008, the County Administrator is responsible for overseeing and coordinating County departments and has authority and responsibility to implement administrative bulletins.

III. **DEFINITIONS.**

a. Cyberattacks. Cyberattacks are digital attacks that are usually aimed at accessing, changing or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

b. Cybersecurity. Cybersecurity is the practice of protecting electronic systems, networks, hardware, software and data from cyberattacks.

c. Cybersecurity defenses. The hardware and software that protect IT assets and data, such as firewalls, network detection and response, and endpoint detection and response.

d. Data breach. A data breach is any security incident in which unauthorized parties gain access to sensitive or confidential information, including personal data such as Social Security numbers, bank account numbers, and healthcare information.

e. Electronic data management plan. Electronic data management plan refers to the plan used by departments to track, manage, and organize their IT assets.

f. Data recovery. Data recovery is the process of restoring lost, corrupted, accidentally deleted or otherwise inaccessible data.

g. Denial-of-service attack. A denial of service (Dos) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber-threat actor.

h. DoIT. DoIT means the Contra Costa County Department of Information Technology.

i. IT assets. IT assets refer to the electronic hardware and software of an entity, such as its applications, servers, mobile phones, network equipment, printers, cameras, computers, and cloud environments.

j. Malware. Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer or a computer system.

k. Phishing. Phishing occurs when a malicious actor sends communications that seem to be coming from trusted, legitimate sources to obtain sensitive information, gain unauthorized access, or malevolently encourage actions by the recipient.

l. Vulnerability management. Vulnerability management is a continuous, proactive, and often automated process that keeps IT assets safe from cyberattacks and data breaches.

IV. **COUNTY DEPARTMENTAL RESPONSIBILITES.** Departments play a crucial role in maintaining cybersecurity. To meet this responsibility, this bulletin provides minimum standards for departments to follow. However, departments should apply higher standards when necessary or prudent.

a. Electronic Data Management. Electronic data management helps to protect the County from data losses, thefts, and breaches by retaining data only as required and ensuring that sensitive data is stored securely. To achieve these goals, County departments shall:

i. develop a management plan for electronic data, which takes into consideration record retention requirements, privacy laws, and the need to securely handle and store sensitive data (see attached Sample Electronic Data Management Spreadsheet); and

ii. keep a current inventory of the department's IT assets. Upon request, DoIT will provide County Departments with an inventory tracking system to help meet this requirement.

b. Security Measures. Security measures help to prevent unauthorized persons from accessing the County's IT assets or causing other harm. In accordance with the need to take such measures, County departments

shall comply with all cybersecurity standards set by DoIT and cooperate with DoIT during cybersecurity audits.

c. Response to Cybersecurity Events. A rapid and planned response to a cyberattack helps to minimize losses, patch vulnerabilities, restore affected systems, and stop the attack. To minimize the effects of these attacks, departments shall do the following:

    i. in accordance with the department's reporting protocol, immediately report suspected cyberattacks to DoIT; and

    ii. establish and maintain data recovery services to restore data following a cybersecurity incident or other disruption to the system. Data recovery services may be established by departments independently or in coordination with DoIT.

d. Training. Because employees can prevent the majority of attempted cyberattacks on IT assets, County employees shall annually take one of the following courses in information security:

    i. an information security training provided by DoIT; or

    ii. a training approved by an employee's department on a topic relating to privacy, data protection, or cybersecurity.

V. **RESPONSIBILITIES OF DOIT.**

a. To assist County departments in maintaining cybersecurity, DoIT shall develop and periodically update cybersecurity standards for the following:

    i. the configuration of departments' IT assets;
    ii. County-developed software;
    iii. minimum acceptable cybersecurity defenses;
    iv. minimum acceptable vulnerability management systems;
    v. contracting with IT vendors and those handling sensitive electronic data and systems; and
    vi. the appropriate level of access to IT assets for a department's employees, contractors, and vendors.

    DoIT shall keep all County departments informed of all cybersecurity standards established and updated by DoIT.

b. To prevent unauthorized persons from accessing the County's IT assets or causing other harm, DoIT shall do the following:

    i. install cybersecurity defenses on County IT assets;

ii. continuously assess, track, and mitigate vulnerabilities to departments' IT assets; and
iii. periodically, but no less than annually, audit the security of departments' IT assets.

The tasks in this subsection (b) may be performed by a department if DoIT and the department determine that the department is better situated to perform these functions and the department uses standards that meet or exceed those set by DoIT.

c. To help detect, understand, and recover from cybersecurity attacks, DoIT shall take the following steps:

i. maintain a countywide log of cybersecurity incidents;
ii. take the lead in coordinating a response to cybersecurity incidents; and
iii. assist in remediation of deficiencies found during cybersecurity incidents and regular security assessments.

VI. **RESPONSIBILITIES OF THE COUNTY ADMINISTRATOR'S OFFICE.** The County Administrator's Office shall be responsible for overseeing compliance with this bulletin.

Related Documents
Sample Electronic Data Management Spreadsheet

Originating Department: Department of Information and Technology

_____
Monica Nino
County Administrator

Document Type	**Retention Period**	**Does it contain sensitive information, e.g., personal information, statutorily protected? If so, what type?**	**Is access to data restricted within the department? If so, to whom?**	**IT system**
Real Property Records. Records documenting the administration, purchase, transfer, or sale of real property including but not limited to deeds, appraisals and valuations, closing statements, agreements, property descriptions, easements, and property dispute documentation.	PERMANENT (Gov. Code, § 34090.)	No	No.	Stored in Shared Drive in Real Property File.
Case files, child welfare. Case files representing EHSD. Specifically, those involving cases of the natural parents of minors scheduled to be removed from the home.	5 years See Gov. Code § 26202; Resol. 2012/XXX	Yes, may include documents filed in the superior court and attorney notes. Welf. & Inst. Code, §§ 827 et seq.	Restricted to juvenile/conservatorship unit unless a need to know shown.	Stored in Shared Drive in Child Welfare File – restricted access.
Case files, probate and conservatorship. Case files representing HSD or EHSD in probate or conservatorship matters.	5 years See Gov. Code § 26202; Resol. 2012/XXX	Yes, may include petitions filed pursuant to the Welfare & Institutions Code §§ 5327, 5350 or 5361. May also include the accounting of use of conservatee's funds, correspondence, court orders, doctor's declaration, ex partes, letters of conservatorship, dismissals, and reappointments.	Restricted to juvenile/conservatorship unit unless a need to know shown.	Stored in Shared Drive in Probate & Conservatorship File – restricted access.

This document is an information security record potentially exempt from disclosure under California Government Code § 7929.210. Please consult County Counsel for any questions about the exemption.