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