COUNTY ADMINISTRATOR

SUSAN S. MURANISHI
COUNTY ADMINISTRATOR

December 1, 2020

Honorable Board of Supervisors
County of Alameda
1221 Oak Street, Suite 536
Oakland, California 94612-4305

Dear Board Members:

SUBJECT: ADOPTION OF THE ALAMEDA COUNTY CYBERSECURITY POLICY

RECOMMENDATIONS:

A. Adopt the Alameda County Cybersecurity Policy; and

B. Authorize the Chief Information Officer in partnership with the County Administrator to implement the new Alameda County Cybersecurity Policy and amend as necessary to protect the County's information assets.

DISCUSSION/SUMMARY:

Cybersecurity is defined as the protection of internet-connected systems, including hardware, software, and data, from cyberattacks. Cybersecurity requires heightened attention at a time when government agencies at home and abroad have fallen victim to coordinated malicious attacks and suffered financial and reputational losses as a result. The COVID-19 pandemic and other events have accelerated the move to more virtual services and remote work, which increases the potential for malicious activity. Adapting to new business practices and implementing virtual business models has increased the need to provide access to the County's information assets from any location securely.

To protect the County's information assets, it is imperative to have a consistent approach to implementing, maintaining, and enhancing cybersecurity capabilities. This begins with having a single, countywide cybersecurity policy that provides direction and establishes the framework for all agencies/departments to follow as they implement technologies to support their business and operational objectives.

The primary objectives of the Alameda County Cybersecurity Policy include:

- Placing the responsibility of cybersecurity for the County with the Chief Information Officer (CIO) who, together with the County Administrator, can establish standards, policies, guidelines, and technology platforms to secure the information assets of the County. The CIO and the Information Technology Department (ITD) have the resources, skills, and exposure to the latest information to help establish consistent and effective approaches that address the evolving cybersecurity risk landscape.

- Increasing the consistency and speed to address the accelerated pace of technology change and the corresponding increase in cybersecurity risk. Recent cybersecurity attacks and financial loss have highlighted the importance of keeping technology platforms current through patching and system upgrades. Even one vulnerable system can allow a malicious actor to access critical technology resources, which can potentially have broad impact throughout the County. It is imperative that potential threats are identified and acted upon quickly to minimize the probability of an attack and reduce the impact when an attack does occur.

- Communicating to all agencies/departments the critical role they play in addressing cybersecurity risk with their employees. This includes complying with countywide technology standards, ensuring employees complete security awareness training, reviewing new technology initiatives with ITD to identify potential security risks, and maintaining awareness of potential cybersecurity threats in their own areas of responsibility.

Given the increasing importance of technology as a critical component to the infrastructure of service delivery to the residents of Alameda County, establishing this countywide Cybersecurity Policy will help promote the continued effectiveness and safety of these technology solutions.

FINANCING:

There is no increase to net County cost as a result of your adoption of the Cybersecurity Policy.

VISION 2026 GOAL:

The Alameda County Cybersecurity Policy meets the 10X goal of **Accessible Infrastructure** in support of our shared vision of a **Healthy Environment.**

Very truly yours,

Susan S. Muranishi
County Administrator

Tim Dupuis
Chief Information Officer

cc: All Agency/Department Heads

COUNTY OF ALAMEDA

Cybersecurity Policy

A. Purpose

The Alameda County Cybersecurity Policy shall be used by Alameda County Agencies and Departments to secure information assets and to help prevent cybersecurity attacks.

This Policy appoints the Chief Information Officer and the Information Technology Department in partnership with the County Administrator as being responsible for defining and developing the policies, roadmaps, standards, tools and technologies to address cybersecurity risks for all Alameda County Agencies and Departments.

This Policy provides for consistent cybersecurity behavior across County Agencies and Departments, as well as provides guidance to information owners on how their information assets should be secured.

This Policy recognizes that all employees play a key role in online safety and the importance of taking proactive steps to enhance cybersecurity at home and in the workplace.

B. Background/Discussion

The need for a countywide Cybersecurity Policy is driven by several factors:

- Dramatic increase in virtual services and remote work
- Rapid technology change
- Increase in malicious activity
- Need for technology and cybersecurity expertise
- Policy drives consistent behavior

Dramatic Increase in Virtual Services and Remote Work

The COVID-19 pandemic drove a rapid and prolonged change in the way the County delivers services to its residents, and in the way work is conducted by County employees. These changes increase the dependency on technology to support business processes and increase the need to provide access to the County's information assets from any location securely.

Rapid Technology Change

Technology changes rapidly, and the pace of change continues to increase. This creates great opportunities for leveraging new technologies to improve the services delivered to Alameda County residents. These include technologies like: Internet of Things (IoT), cloud computing, unified communication, collaboration tools, and social networking, to name a few. However, while there are many benefits from these new technologies, new skills are required to support them, and they have opened new opportunities to exploit vulnerabilities and gaps for malicious purposes.

Increase in Malicious Activity

As these technologies increase in sophistication, so has the frequency and impact of malicious attacks. Examples of significant cybersecurity breaches have increased significantly in the last few years, and the diversity and impact of these incidents are growing. The types of issues facing commercial and government entities include ransomware, phishing, credential and identity theft, denial of service, and data exfiltration, among others.

Need for Cybersecurity Expertise

Preparing for and responding to business disruptions stemming from cybersecurity attacks has become a crucial capability for IT organizations. Developing a comprehensive technology and cybersecurity program requires knowledge, skills, and experience that go beyond typical IT support functions. In Alameda County, the responsibility for defining and developing the

technology policies, standards, tools, and technologies to address these risks lies with the Chief Information Officer and the Information Technology Department, which has the resources and expertise to meet this responsibility.

Policy Drives Consistent Behavior

Policies are an important tool to help guide organizations toward the establishment of efficient and secure systems that users can and do depend on every day to make decisions. Having Information Technology policies built on government and industry best practices will help ensure that Agencies and Departments are making their systems safe and reliable for all stakeholders and ensuring that services are delivered in the most cost effective and secure manner. Policies also help drive consistent behavior across organizations which reduces risk and increases efficiencies.

This Policy is aligned with best practices for state and local governments and was developed as a collaborative effort between the Information Technology Department (ITD) and the County Administrator's Office (CAO). It is intended to provide guidance to Alameda County Agencies and Departments and provide the basis for developing and maintaining additional policies, standards, guidelines, and procedures cybersecurity.

C. Policy

This Policy applies to the procurement, development, implementation, operations, and maintenance of information technology assets for all County entities.

It is the Policy of Alameda County that:

- The Chief Information Officer (CIO), in collaboration with the County Administrator, has responsibility for establishing policies and standards related to technology and cybersecurity;
- The CIO shall be responsible for ensuring that all technology assets, including hardware, software, cloud services, or other information assets comply with the County technology and cybersecurity policies and standards;
- The Information Technology Department (ITD) will be responsible for the identification, procurement, implementation, operations and maintenance of all cybersecurity related tools and products including hardware, software and cloud services;
- ITD shall have visibility into all devices connected to the County network permanently or periodically using technology defined by the Information Technology Department;
- ITD shall be responsible for ensuring that all devices connected to the County network permanently or periodically are updated with current security patches and operating systems on a timely basis or the devices will be removed from the network;
- ITD will keep current on all technologies required to protect the County's Information Assets;
- ITD, in partnership with the General Services Agency, shall provide oversight for procurement of new technology systems and products and include review of such systems and products for compliance with County cybersecurity policies and standards;
- Agencies and Departments will report all suspected IT device-related malicious activities and attacks to ITD immediately;
- Agencies and Departments will ensure all devices accessing the County's Information Assets comply with the cybersecurity policy and standards defined by ITD;
- Agencies and Departments will ensure all staff take Security Awareness Training as administered by ITD;
- Any deviation from this policy will require the Alameda County Agency or Department to obtain Board of Supervisors approval.

D. Agency/Department Discretion

Each Agency or Department is required to understand and comply with the Countywide Cybersecurity policies and standards established by the Information Technology Department and the County Administrator. Agencies/Departments can develop their own policies and standards for their specific needs so long as they comply with and support the Countywide Policy and any additional policies and standards defined by the Information Technology Department and the County Administrator.

E. Conclusion

This Policy is intended to protect Alameda County's technology and information assets by promoting consistent behavior across County Agencies and Departments, as well as providing guidelines to information owners on how their technology and informational assets can and should be managed and secured.

F. Definitions

Cloud Computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Collaboration Tools are technologies that promote the exchange of information among teams and individuals to promote innovation, idea-generation, and productive teamwork.

Credential and Identity Theft is a type of cybercrime that involves stealing a victim's proof of identity. Once credential or identity theft has been successful, the attacker will have the same account privileges as the victim.

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

Data Exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various techniques, typically by cybercriminals over the Internet or other network.

Denial of Service is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Information Assets are organized information and business data that is valuable and easily accessible to those who need it. Information Assets comprise a wide range of data, product, services, and process information.

Internet of Things (IoT) is the network of interconnected devices which are embedded with sensors, software, network connectivity, and necessary electronics that enables them to collect and exchange data making them responsive.

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

Security Patch is a software or operating-system patch that is intended to correct a vulnerability to hacking or viral infection.

Social Networking is the use of dedicated websites and applications to interact with other users, or to find people with similar interests to oneself.

Unified Communication is the system that integrates (or “unifies”) multiple communication methods within a business. For example, integrates with phone calls, video conferencing, instant messaging, email, SMS, fax, to name a few.

G. Document History

Version #	Date	Author/Editor	Description of Changes
1.0	12/04/20	ITD	Original