Monterey County

Subject:	Security Policy
Date Issued:	May 13, 2014
Revision Date:	August 31, 2021
Issued by:	Information Technology Governance Committee
Approved by:	The County of Monterey Board of Supervisors
Applies to:	All County Officials, Employees and Affiliates

Table of Contents

1. INFORMATION TECHNOLOGY SECURITY POLICY

1.1. POLICY PURPOSE

The purpose of this policy is to establish County-wide information security practices which protect and secure County information and information technology resources from intrusion and misuses, as required by California and federal law and as recommended by industry best practices.

1.2. POLICY SCOPE

This policy applies to all County employees and affiliates.

1.3. DEFINITIONS

1.3.1. Affiliates – Includes but is not limited to, third party contractors, volunteers, advisory and other committee and commission members, vendors, or others associated with the County in order to accomplish County business.

1.3.2. Information Owner - The official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Generally, this role falls upon a Department Head.

1.3.3. Information Technology Resource - All computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources. The components may be individually controlled (i.e., assigned to an employee) or shared in a single-user or multi-user manner; they may be stand-alone or networked; and they may be stationary or mobile.

1.3.4. Information Security Team – A team of individuals who work for and report directly to the Chief Security and Privacy officer and assist in executing the Chief Security and Privacy Officer's responsibilities as directed.

1.3.5. Business Associate Agreement – A written agreement to refrain from using or disclosing department information other than as permitted or required by the Agreement or as required by law and to use current industry safeguards to prevent use or disclosure of department information covered by the agreement or as required by law.

1.3.6. Computer – Any computing resource that accesses, stores or otherwise provides connectivity to County information, including but not limited to devices such as desktop computers, servers, smart phones, tablets and laptops.

1.4. ROLES AND RESPONSIBILITIES

The County has established the following Information Security roles and responsibilities:

1.4.1. **Chief Security and Privacy Officer (Chief Security and Privacy Officer)**. To achieve the goals of this Policy, a Chief Security and Privacy Officer position shall be maintained within the County. The County Board of Supervisors authorizes the County's Chief Security and Privacy Officer to develop and maintain the County's Information Security Program and requires all County Departments to comply. Specific guidance, direction, and authority for information system security are centralized for the County and its

subsidiaries in the role of the Chief Security and Privacy Officer. The Chief Security and Privacy Officer shall:

1.4.1.1. Implement, administer, and interpret County Information Security Policies

1.4.1.2. Establish and maintain Information Security Standards in support of Information Security Policy, laws and regulations. Standards consist of specific low level mandatory controls that help enforce and support the information security policy

1.4.1.3. Establish, provide and maintain Information Security guidelines and best practices. Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place

1.4.1.4. Oversee the assessment of Information Security risks and oversee policy, legal and regulatory gap analyses with the assistance, as requested, of County Counsel

1.4.1.5. Recommend technologies, practices and appropriate corrective actions to mitigate Information Security risks

1.4.1.6. Review and assess the risk of technical changes that affect County security posture

1.4.1.7. Promote County-wide information security awareness

1.4.1.8. Interpret laws and regulations as they apply to County information security practices

1.4.1.9. Adopt best practices and recommendations from agencies such as NIST, CERT, SANS, DOD, and implement as necessary to preserve information technology resources and information

1.4.1.10. Oversee the security and intrusion monitoring of the County's networks

1.4.1.11. Oversee a Security Incident Response Team as a multi-disciplinary organized team that is trained to respond to major security incidents

1.4.1.12. Oversee information technology-related forensic investigations as directed by County Counsel, the District Attorney's Office, or a law enforcement agency

1.4.1.13. Audit compliance with County Information Security Policy and Standards and provide vulnerability assessment and reporting for the purposes of:

Fulfilling the County Board of Supervisors' Response to the Monterey County Civil Grand Jury 2004 Final Report, which stipulates that the Chief Security and Privacy Officer have access to all systems for the purpose of auditing compliance with the Board's adopted policies, security incident investigation and response, and counsel-directed investigation activities,

1.4.1.13.1. The Chief Security and Privacy Officer shall have comprehensive around-the-clock system administrator/superuser rights to all network-connected County devices except for standalone un-networked County devices, or those County devices attached only to an isolated LAN.

1.4.1.13.1.1. For the purpose of this Policy, an isolated LAN is defined as a network for which all connectivity is contained to a single building and limited to use by a single department, affording the network and its connected devices protection by physical security measures. Physical access to these standalone un-networked computers and isolated LANs shall be provided to the Chief Security and Privacy Officer on request.

1.4.1.13.1.2. Unless written direction has been issued by County Counsel, the District Attorney's Office, or a law enforcement agency, physical access to computers shall be coordinated with the appropriate department

information owner(s) (defined in section 1.4.2). Physical access may be restricted where limited by law, regulation or written departmental policy.

1.4.1.13.1.3. No department information shall be intentionally accessed without the written direction of the County Counsel's office, the District Attorney's Office, a law enforcement agency, or the affected department(s).

1.4.1.13.1.4. The access granted to the Chief Security and Privacy Officer shall not be utilized to grant similar access to anyone outside of the Chief Security and Privacy Officer's Information Security team.

1.4.1.13.1.5. The Information Technology department shall enter into Business Associate Agreements with departments whose information is protected by law so that in the event of any incidental contact with that protected information, the Information Technology department shall be accountable to maintain the confidentiality and privacy required to meet applicable laws and regulations.

1.4.1.14. Maintain a separation-of-duties security program. While the Chief Security and Privacy Officer shall partner with County departments toward their success and the fulfillment of their business goals, the Chief Security and Privacy Officer shall not control the IT business nor possess the authority or responsibility for the support and maintenance of the day-to-day production IT environment. By maintaining a "separation of duties" security program, the Chief Security and Privacy Officer shall be able to both advise the County and audit its security as well. The Chief Security and Privacy Officer shall be responsible, however, for overseeing the compliance of the IT department with County Policies, Standards and best practices.

1.4.1.15. Have appropriate staff and effect appropriate security management under the authority of the Director of Information Technology and the County Administrative Officer.

1.4.1.16. Collaborate with and coordinate departmental information protection actions with the County's departmental Information Security Officers.

1.4.2. **Information Owners**. Information owners shall:

1.4.2.1. Maintain both the physical and logical security of the information technology resources and information under their jurisdiction.

1.4.2.2. Ensure the classification of data is defined and designated in a manner consistent with County data classifications.

1.4.2.3. Periodically conduct a risk assessment of each information technology resource for which they are responsible to determine both risks and vulnerabilities.

1.4.2.4. Ensure, for the information utilized, stored, and accessed by their departments, that security measures are implemented which are appropriate to the level of protection required by policy and law.

1.4.2.5. Maintain information access controls over department information. In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

1.4.3. **Director of Information Technology**. The Director of Information Technology shall:

1.4.3.1. Establish and maintain County-wide information security policies.

1.4.3.2. Act as the County's Change Control Agent. No changes to the County's information infrastructure shall be executed without the Change Control Agent's knowledge and approval.

1.4.3.3. Maintain safeguards for the information technology resources and information under the Director of Information Technology's jurisdiction.

1.4.3.4. Review and approve or deny exceptions to this Policy.

1.4.4. **Department of Information Technology**. The Department of Information Technology shall:

1.4.4.1. Provide technical guidance to all County departments.

1.4.4.2. Under the direction of the Chief Security and Privacy Officer, maintain a Security Incident Response Team to respond to virus infestations, hacker intrusions, and similar events.

1.4.4.3. Review proposals for new services, hardware and software, networks, external connectivity, or other systems for communicating information for compliance with County Information Security Policy and Security Standards, and shall consult appropriate County businesses for business-specific regulatory requirements and applicable legal mandates.

1.4.4.4. Review County participation in external networks, or as a provider of services that external parties rely on, for compliance with County Information Security Policy and Security Standards.

1.4.5. **Departmental Information Security Officers (ISOs)**. Each Department Head, in coordination with the Chief Security and Privacy Officer, shall nominate an individual to serve as that Department's Information Security Officer. The Departmental Information Security Officer shall:

1.4.5.1. Be a full time County employee.

1.4.5.2. Not directly report to the Chief Security and Privacy Officer

1.4.5.3. Collaborate with and coordinate departmental information protection actions with the Chief Security and Privacy Officer. The responsibilities of the Departmental Information Security Officers encompass all information for which the department has administrative responsibility. They are responsible for ensuring adherence to procedures, guidelines and safeguards that are required to protect information, confidentiality and privacy rights, and to ensure integrity, auditability, and controllability of the information resources within the department.

1.4.5.4. Monitor departmental compliance with County Security Policy, County Security Standards, Information Security best practices, business-specific regulatory requirements, and applicable legal mandates, as applied to the particular business and/or mission of County departments.

1.4.5.5. Secure and maintain the confidentiality and integrity of protected information within the department by reviewing all security considerations for the department's automated and manual processes in coordination with County Security Policy, County Privacy Policy, County Security Standards, Information Security best practices, business and/or mission-specific regulatory requirements, and applicable legal mandates.

1.4.5.6. Work with the Chief Security and Privacy Officer and Information Security Staff to analyze department information environments on an ongoing basis to identify risks arising from changes in those environments.

1.4.5.7. Serve as the initial security point of contact for their department's employees.

1.4.5.8. Work with the County's Security Incident Response Team, report all Information Security incidents to the Chief Security and Privacy Officer, and investigate the authenticity of reported security violations in coordination with the Chief Security and Privacy Officer and the Security Incident Response Team before initiating corrective actions within their department.

1.4.6. **Department Managers and Supervisors**. Department Managers and Supervisors shall:

1.4.6.1. Ensure that employees under their supervision implement security measures as defined in County Security Policies and Standards and as appropriate to their data classifications.

1.4.6.2. Inform employees under their supervision of information security issues and promote overall security awareness.

1.4.6.3. Enforce compliance with County Information Security Policy and Information Security Standards.

1.4.6.4. Conduct entry or pre-exit security clearance processes upon employment or termination of employment of officers or employees or fulfillment of contractual agreements.

1.4.7. **County Officers and employees**. All County Officers, employees and affiliates working for or doing business with the County shall:

1.4.7.1. Do no harm to nor attempt to harm or steal any County information resource or information resource.

1.4.7.2. Know and follow County Policies and Standards, and apply best practices pertaining to protected information and information security.

1.4.7.3. Prohibit unauthorized individuals from obtaining access to County information technology resources and information and access only the information for which he/she is authorized in the course of normal business activity.

1.4.7.4. Maintain exclusive control over and use of his/her password or other authentication mechanism and protect it from inadvertent disclosure to others.

1.4.7.5. Ensure that information under his/her control and/or direction is safeguarded according to its data classification.

1.4.7.6. Report to his/her supervisor or Departmental Information Security Officer any incident that appears to compromise the security of County information resources.

1.4.7.7. Complete information security awareness training annually.

1.5. ACCEPTANCE OF RISK AND RESPONSIBILITY

1.5.1.1. The security of the County's information technology resources and information is the responsibility of all County employees.

1.5.1.2. Information security risk decisions are assigned to, and are the responsibility of the County departments whose information is the target of the particular risk. When presented with a Chief Security and Privacy Officer-directed or approved security risk assessment of an existing or proposed change or service, information owners shall review the risks to their information technology resources and information from the identified security risks and security gaps, and either:

1.5.1.2.1. Accept the risks to their information; or

1.5.1.2.2. Execute Information Security's recommendations and/or other mitigation steps in order to reduce the risk to an acceptable level; or

1.5.1.2.3. Transfer the risks as necessary.

1.5.1.3. The County Administrative Officer, their designee, and/or the County Board of Supervisors shall be responsible for any information or information technology resource risk decisions where the risk applies to a significant portion of the County or to the entire County as a whole.

1.6. **STANDARDS**

1.6.1. In addition to County Information Security Standards documents established and maintained by the Chief Security and Privacy Officer, the County shall adopt the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework). This Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. This Framework is the basis for the County's required annual Nationwide Cybersecurity Review self-assessment, designed to measure the gaps and capabilities of state, local, tribal and territorial governments' cybersecurity programs.

1.7. **ACCESS CONTROL**

1.7.1. Access to County information technology resources and information shall be authorized by the information owners.

1.7.2. Wherever technically feasible, all access to information shall be granted according the National Institute of Standards and Technology's Role Based Access Control (RBAC) and Role Based Security models. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles.

1.7.3. Every software program and every user of any County system or network shall operate using only privileges necessary to complete the job. The computer and communications system privileges of all users, systems, and software shall be restricted based on the need-to-know. Systems, files and user permissions shall begin in a closed state and shall only be opened to those whose role requires access. Default access settings shall be configured for denial-of-access and opened thereafter as necessary to accomplish County business purposes.

1.7.4. Regarding Access Authorization:

1.7.4.1. Requests for new User IDs, role and privilege changes for County officers and employees shall be requested by the user's manager.

1.7.4.2. Requests for new User IDs, role and privilege changes for individuals who are not County officers or employees shall be requested in writing by the department head or authorized representative sponsoring the work activity that necessitates access.

1.7.4.3. All users shall sign a compliance statement indicating the user understands and agrees to abide by County Policies, Standards and procedures related to access to County computers and networks. Users must receive a copy of these policies, standards and procedures and sign that they have received these copies.

1.7.4.4. Documentation reflecting user access requests and changes shall be retained for a period of at least one year.

1.7.4.5. All user-IDs shall automatically have their associated privileges revoked after 30 days of inactivity. Automatic suspension shall include notification to the assigned department for information and recommendations.

1.7.4.6. Privileges granted to users who are not County officers or employees shall be granted for periods of 90 days or less. As needed, users who are not County officers or employees shall have their privileges reauthorized by the sponsoring department head every 90 days.

1.7.5. All access rights and privileges granted to users shall be re-evaluated on an annual basis by management. In response to feedback from management, all access rights and privileges no longer needed by users shall be promptly revoked.

1.8. AUDIT

1.8.1. Scope

1.8.1.1. This policy applies to all County employees and affiliates. This covers all computer and communication devices owned or operated by the County. This also covers any computer and communications devices that are present on County premises or used for County business, but which may not be owned or operated by County. This also applies to any computing resource that accesses, stores or otherwise provides connectivity to County resources, including personal devices such as smart phones, tablets and laptops. Unless contractual agreements dictate otherwise, messages sent over County computer and communications systems are the property of the County. To properly protect and manage this property, management reserves the right to examine all information stored in or transmitted by these systems. County employees and personnel of affiliates shall have no expectation of privacy associated with the information they store in or send through these systems.

1.8.2. Requirements

1.8.2.1. Compliance with County Policies and Standards shall be regularly (not less than annually) audited by the Information Security Team. Audits may be conducted to:

1.8.2.1.1. Ensure integrity, confidentiality, and availability of information and resources. Confidentiality is about protecting the information from disclosure to unauthorized parties. Integrity is protecting information from being modified by unauthorized parties. Availability refers to ensuring that authorized parties are able to access the information when needed. For information specific to a particular department, this auditing task may be delegated to the department's Departmental Information Security Officer.

1.8.2.1.2. Investigate possible security incidents to ensure conformance to County security policies

1.8.2.1.3. Monitor user or system activity where appropriate

1.8.2.1.4. Verify that vulnerability management is being maintained at the appropriate security level

1.8.2.1.5. Verify that malware and other system protections are being maintained at current levels

1.8.2.1.6. Validate compliance with stated security policies.

1.8.2.2. All information technology resources throughout the County shall be accessible and auditable by the Chief Security and Privacy Officer per the details in section 1.4.1.13.1.

1.9. COMPUTER SECURITY

1.9.1. DEFINITIONS

1.9.1.1. Shareware – Shareware (also termed trialware or demoware) is proprietary software that is provided to users on a limited basis and sometimes only for certain limited trial basis and pursuant to a license which restricts any commercial benefit, use or exploitation of the software.

1.9.1.2. Open Source Software – Open-source software (OSS) is computer software with its source code made available and licensed in such manner that the copyright holder provides the rights to study, change and distribute the software to anyone and for any purpose.

1.9.1.3. Freeware - Freeware (a hybrid of "free" and "software") is software that is available for use at no monetary cost or for an optional fee, but usually (although not necessarily) closed source with one or more restricted usage rights.

1.9.1.4. Ransomware – Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

1.9.2. County computers shall only be used in a secure environment. An environment is secure when appropriate controls have been established to protect computer software, hardware, and information. These controls shall provide a measure of protection commensurate with the classification of the data and the assessed risks.

1.9.3. Secure user identification and authentication shall be used on all devices, applications and systems software.

1.9.4. All County computing and network-connected devices shall utilize an access control system that provides privilege control as well as change control, and shall employ software which restricts access to the files of each user, logs the activities of each user, and has special privileges granted to a systems administrator. Portable computers and home computers which contain County information are also covered by this policy.

1.9.5. All County computing and network-connected devices shall be as fully protected as possible from malicious computer hacking and all forms of malware including computer viruses, worms, trojan horses, rootkits, bots, ransomware, crimeware and all other malicious and unwanted software, including new types not listed here. These systems shall be regularly examined to assure their compliance with this policy.

1.9.6. All software running on devices connected to the County's network shall utilize the latest security updates provided by the software vendor or the County as addressed in County standards.

1.9.7. County computers and networks shall only run trusted software that has been approved by a Department Head or departmental Information Security Officer. Trusted software includes software from business partners, knowledgeable and trusted user groups, well-known systems security authorities (such as SANS), computer or network vendors, or commercial software vendors. Software downloaded from the Internet, shareware, open source software, freeware and other software from un-trusted sources shall not be used unless it has been approved in writing by the department's Information Security Officer and the Chief Security & Privacy Officer has been notified. In instances where concerns

exist regarding the use of particular software, the Chief Security & Privacy Officer may require a formal risk assessment be completed. Users shall not download or install any unapproved software on any County device.

1.9.8. The use of a "personally-owned" computer or mobile computing device such as tablets, smartphones, etc., or any of its component parts to connect to the county network or access internal county resources shall be permitted only after permission has been granted by the employee's Departmental Information Security Officer (ISO) and the appropriate policy and acceptable use forms have been completed.

1.9.8.1. In the event of a security issue with a "personally-owned" device, the owner of the device is required to remediate all issues before utilizing the device to access any county resources.

1.9.9. Buildings which house County information technology resources shall be protected with physical security measures that prevent unauthorized persons from gaining access to the equipment and that lessen the risks of theft, destruction, and/or misuse.

1.9.10. All County servers and network equipment shall be physically secured and be placed in locked cabinets, locked closets, or locked computer rooms.

1.9.11. The Information Technology Department shall create and maintain a list of managers who are authorized to control and grant access to County facilities that contain information technology resources.

1.9.12. County Departments shall maintain records of the persons currently and previously inside the non-public areas their facilities.

1.9.13. Inventory records of computer equipment shall be kept up-to-date. The master inventory shall be maintained by the Department of Information Technology, with the assistance of the individual departments, in conformance with the adopted Information Technology Resources Management policies.

1.9.14. The loss or theft of any computer hardware and/or software shall be reported as soon as practical to the department's Information Security Officer (ISO) and the ITD Service Desk.

1.10. **IDENTIFICATION AND AUTHENTICATION**

1.10.1. All computers shall have, at minimum, password access controls that limit access to users with unique user ids and passwords.

1.10.2. Wherever technically possible, all County applications and services shall utilize a single centralized, single sign-on, identity management and authentication source.

1.10.3. For County applications and services that are available for login on the Internet, the application or service shall be configured so that an outside attacker with a stolen password cannot login to the service.

1.10.4. Each user shall positively identify themselves as individuals with authorizations that are unique to each individual user.

1.10.4.1. Generic, guest or universal IDs are not permitted without a signed acceptance of risk by the Department Head or designee.

1.10.5. Initial authentication assigned to new users or authentication (such as passwords) changed by third-party reset shall be changed by the user at the user's next login.

1.10.6. Default or vendor-supplied authentication (such as passwords) shall be changed before placed into production.

1.10.7. User authentication information (such as passwords) shall never be disclosed to or shared with anyone or be exposed in openly viewable form.

1.10.8. All changes of user-IDs shall be logged.

1.10.9. Passwords shall be long, unpredictable and difficult to guess.

1.10.10. Every log-in banner must include a special notice. This notice must state:

1.10.10.1. The system is to be used only by authorized users.

1.10.10.2. By continuing to use the system, the user represents that he/she is an authorized user.

1.10.10.3. All activities on the system shall be monitored.

1.10.10.4. Users shall have no expectation of privacy.

1.10.11. Systems and applications must not divulge information about the County or grant access to information until after a valid user login.

1.11. SECURITY LOGGING

1.11.1. Users shall be put on notice about the specific acts that constitute computer and network security violations. Users shall also be informed that such violations will be logged. Refer to the County's Appropriate Use Policy for more details.

1.11.2. County computer and communications systems shall securely log all significant security events. Security events include but are not limited to:

1.11.2.1. Account logon events

1.11.2.2. Account management

1.11.2.3. Users switching user-IDs

1.11.2.4. Password guessing attempts

1.11.2.5. Changes to user privileges

1.11.2.6. Electronic configuration policy changes

1.11.2.7. Attempts to use unauthorized privileges

1.11.2.8. Attempts to access unauthorized objects

1.11.2.9. Modifications to production application software

1.11.2.10. System events and modifications to system software

1.11.2.11. Changes to logging subsystems

1.11.3. Logs containing security relevant events shall be securely retained by the Information Technology Department for at least three (3) months.

1.11.4. These logs shall be viewed daily and in a timely manner by assigned Server Administrators, Information Owners, or assigned Information Technology staff.

1.12. NETWORK SECURITY

1.12.1. Description

1.12.1.1. The County must comply with the requirements of the California Department of Justice, the requirements under FBI Criminal Justice Information System security

policies, and the requirements of the California Law Enforcement Telecommunication System. As a result of these and other requirements, strict controls over the security of the County network are necessary.

1.12.2. **Requirements**

1.12.2.1. No changes to the County's data networks shall occur without the expressed knowledge and consent of the Information Technology Department.

1.12.2.2. New types of connections between two or more County computer systems or networks shall not be established unless such approval has first been obtained in writing from the Director of Information Technology.

1.12.2.3. The bridging of County networks or the participation in external networks as a provider of services that external parties rely upon shall be expressly prohibited unless explicitly permitted by the Director of Information Technology in writing. Bridging is defined as the simple act of using a computing device to create a connection between a foreign network and the local County network at the same time. Examples of "bridging of the County network" include, but are not limited to:

1.12.2.3.1. Connecting a live modem to a network-connected County computer.

1.12.2.3.2. Connecting a FAX machine to the County network.

1.12.2.3.3. Connecting to a County computer from a remote location using means in violation of County Security Standards.

1.12.2.3.4. Connecting from a County computer to a computer or network on the Internet using VPN or other remote-control mechanisms in violation of County Security Standards.

1.12.2.3.5. Connecting alternative access to the Internet to the County network or a network-connected County computer or device.

1.12.2.3.6. Connecting the County network or a network-connected County computer to any third-party network using means in violation of County Security Standards.

1.12.2.3.7. Connecting a wireless device to the County network that concurrently is connected to a third-party provider network

1.12.2.4. As processes deployed across a local or wide area network can result in a negative impact on overall network performance, controlled testing of network processes shall be conducted before being deployed. Processes that have negative impact on the network shall not be deployed until performance issues are coordinated and network performance issues have been addressed.

1.13. SECURITY PERIMETER

1.13.1. Purpose

1.13.1.1. This section establishes essential policies and operational requirements for Security Perimeter Architecture (the Security Perimeter).

1.13.2. Scope

1.13.2.1. This applies to all resources, systems, connectivity, and services as defined within the Security Perimeter and to all entities located on the County's Wide Area Network. Furthermore, it applies to all County employees, officers, and affiliates, including all personnel affiliated with third parties participating in any capacity within the County's

defined Security Perimeter environment. Existing legal requirements shall not be superseded by this policy.

1.13.3. **Description**

1.13.3.1. The Security Perimeter is an essential and critical Wide Area Network component and is crucial to the security of County infrastructure and information systems. The Security Perimeter is defined as the "managed point of entry/exit" to County infrastructure resources. It includes but is not limited to all County Firewalls, Intrusion Prevention Systems, Public Service Networks (also referred to as Demilitarized Zones, or DMZ's), Virtual Private Networks (VPN), remote connectivity resources, cloud-based infrastructure, and the network architecture resources providing connectivity for the environment.

1.13.3.2. This section defines the requirements which apply to components of the Security Perimeter; both the logical and physical. This does not replace or supersede overarching Security Policies which address overall development of network deployment, but rather focuses on critical components establishing the stability and security of the Security Perimeter.

1.13.3.3. The Security Perimeter is divided into two categories; its logical components and its physical components.

1.13.4. **Logical Components**

1.13.4.1. Definitions

1.13.4.1.1. Logical components refer to the logical representation of how the Security Perimeter is viewed, and include, but are not necessarily limited to:

1.13.4.1.1.1. Internet

1.13.4.1.1.2. Intranet: Connectivity of the security perimeter to the Intranet (the County's Wide Area Network, or WAN) provides County access to external resources foreign to the County's WAN.

1.13.4.1.1.3. Extranet: Connectivity to business partners, vendors, external connectivity to other private networks

1.13.4.1.1.4. Public Service Network (also called a De-militarized Zone, or DMZ): Secured zones that protect resources from full exposure to any connection (Internet, Extranet, Remote Access, Intranet, etc).

1.13.4.1.1.5. Remote Access: remote access connectivity such as dial-up networking and/or Virtual Private Networking (VPN) that is utilized to gain privileged access to County Infrastructure systems.

1.13.4.2. Applicable Policies

1.13.4.2.1.1. The point(s) of logical component connectivity shall be noted as such as well as be visually auditable.

1.13.4.2.1.2. Any logical perimeter component connections shall connect to a County firewall or similar security device and shall be managed by the Information Technology Department.

1.13.4.2.1.3. Where possible, disparate business partners or Extranets shall be secured and protected from each other

1.13.4.2.1.4. Where possible and appropriate, the network addresses of hosts and all other information not necessary to disclose shall be masked or hidden.

1.13.4.2.1.5. Placement of resources within a Public Service Network shall adhere to an established IT procedure.

1.13.4.2.1.6. Public Service Network hosted resources shall adhere to the requirements in County Information Security Standards.

1.13.5. **Physical Components**

1.13.5.1. Definitions

1.13.5.1.1.1. Firewalls: those devices which apply rules or filters to network traffic

1.13.5.1.1.2. Routers and Switches: those devices which provide connectivity and connections points to resources within the Security Perimeter

1.13.5.1.1.3. Remote Access Appliances: those devices which provide remote connectivity to County resources.

1.13.5.1.1.4. Circuits and Connectivity: provide access to foreign resources not part of the County's Wide Area Network. These most commonly include connections to the Internet and Extranet business partners.

1.13.5.2. Applicable Policies

1.13.5.2.1. Physical components, where capable and appropriate, shall be configured in such a manner as to not divulge their function and or location.

1.13.5.2.2. Physical components, where capable and appropriate, shall display warning banners for logon.

1.13.5.2.3. Physical component administrators shall have unique passwords and/or access methods.

1.13.5.2.4. Physical components shall be secured through physical and logical security measures allowing only authorized administrator access.

1.13.5.2.5. Physical components, where capable and appropriate, shall provide for auditing and logging.

1.13.5.2.6. Router(s) and Switch(es), where appropriate, shall leverage additional security functions such as Access Control Lists (ACL) that limit administrative access.

1.13.5.2.7. Unused ports shall remain in an inactive or shut state until required to be activated for connectivity.

1.13.5.2.8. All connections shall be clearly labeled and identifiable.

1.13.5.2.9. All connections shall physically be located in a sight or limited walking auditable radius.

1.13.5.2.10. All circuits shall terminate (county-side) on a County Router in the Information Technology department where possible.

1.13.5.2.11. Any circuits terminating (county-side) on an affiliate router shall then connect to a County managed Router or Firewall.

1.13.6. **Management, Monitoring, and Control**

1.13.6.1. This policy provision governs all resources which comprise the "management environment" of the County's security perimeter. It refers to management consoles or any control device or method used to manage, control, or otherwise configure the security perimeter of the County. The following policies apply:

1.13.6.1.1. All aspects of the County's security perimeter shall be managed by the Information Technology Department.

1.13.6.1.2. Only administrators authorized by the Director of Information Technology shall be granted access to management of the security perimeter.

1.13.6.1.3. An auditable access and transaction history shall be available including logon, access, activities, and surveillance where appropriate.

1.13.6.1.4. No changes to the security perimeter, including devices, systems and services placed on the County's perimeter or in any Public Service Network shall occur without the written authorization of the Chief Security and Privacy Officer or IT Director.

1.13.6.2. No changes to the County's defensive security posture, whether internal or on the security perimeter (including, but not limited to, changes to or the disabling of network firewalls, proxies, application firewalls, malicious website filtering) shall occur without the written authorization of the Chief Security and Privacy Officer or IT Director.

1.14. REMOTE ACCESS

1.14.1. Scope

1.14.1.1. This section applies to all County departments, officers, employees, and affiliates accessing the County network from a remote, non-County network-connected location. This applies to implementations of remote access directed through any type of remote access device or VPN Concentrator.

1.14.2. Definitions

1.14.2.1. Advanced Authentication - authentication that adds an additional layer of security to the standard username and password authentication method.

1.14.3. Description

1.14.3.1. Approved County employees and authorized third parties or affiliates (vendors, etc.) may use the benefits of County remote access. Users are responsible for selecting an Internet service provider (ISP), paying associated fees for these services, coordinating installation, and installing any required software in order to provide the appropriate levels of Internet connectivity so as to participate in the County's remote access services. Additionally,

1.14.3.1.1. All remote access devices enabling access to the County network shall be set up, configured and managed by the Department of Information Technology. All other remote access connections shall be strictly prohibited without the expressed written consent of the Director of Information Technology.

1.14.3.1.2. All remote access connections must come through the Security Perimeter managed by the Information Technology Department.

1.14.3.1.3. All County policies that apply to on-site individuals shall apply to individuals connecting remotely. All individuals are required to comply with County Security Policies and Security Standards whenever connecting to the County's network or working with County information. Resources used to remotely connect to County networks and resources must adhere to the adopted

Security Standards for County-connecting systems. Individuals utilizing remote access are responsible for complying with the County's Security and Appropriate Use Policies and for the security of information at their remote work site.

1.14.3.1.4. By using remote access technology with personal or third-party equipment, individuals understand that their machines are a de facto extension of the County's network and, as such, are subject to the same rules, regulations and legal discovery requirements that apply to County-owned equipment.

1.14.3.1.5. All County employees working remotely shall comply with any existing County Telecommuting Policies.

1.14.3.1.6. All remotely-connecting individuals shall be aware of the types and classifications of data they are working with and the legal, regulatory and policy requirements regarding the handling, transmission and storage of such data.

1.14.3.1.7. Users of computers connecting to the County's network shall configure their computers to comply with the County's Security Policies and Security Standards and shall actively protect the County's network from harm or intent to harm.

1.14.3.1.8. All remote access users shall ensure that unauthorized users are not allowed access to the County's networks.

1.14.3.1.9. Remote access sessions utilizing the Internet as the means of connectivity shall be encrypted.

1.14.3.1.10. Remote access shall be controlled using either advanced authentication, a one-time password mechanism (such as a token device), or a public/private encryption key system with a strong passphrase and back-end authentication, or a similar, more secure method.

1.14.3.1.11. Remote access to County networks is limited to circumstances where access is required for legitimate business. In the case of County employees where remote access may be granted to the entire County network, advanced authentication shall be utilized to gain access.

1.14.3.1.12. When actively connected to the County network, remote access devices shall force all traffic to and from the remote PC over the connection to the County. All other traffic will be dropped. Dual (split) tunneling shall not be permitted; only one network connection shall be allowed.

1.14.3.1.13. No bridging of the County's network to any other network shall be allowed at any time. Bridging is defined as the simple act of using a computing device to create a connection between a foreign network and the local County of Monterey network at the same time. County network resources are only available to the remotely connecting device via the authorized connection provided and shall never be shared with other devices and networks.

1.14.3.1.14. The use of modems is prohibited unless approved by the Director of Information Technology.

1.14.3.1.15. Approved modems that are utilized for vendor remote maintenance on County computer and communication systems shall be disabled until the specific time they are needed by the vendor. These ports shall be disabled after use. Alternatively, dial-up connections can be established with vendors via outbound calls initiated by County employees.

1.14.3.1.16. Remote access users shall be automatically disconnected from the County's network after 20 minutes of inactivity. Pings or other artificial network processes shall not be used to keep the connection open.

1.14.3.1.17. Only approved remote access client software shall be used.

1.14.3.1.18. Users shall not connect to the County network while using an unprotected or unauthorized wireless network, unless VPN is used.

1.14.3.1.19. Remote access sessions shall be monitored and logged.

1.14.3.1.20. All inter-processor commands from non-County locations are prohibited unless a user or process has first logged-in. Examples of such commands are remotely-initiated requests for a list of users within the County or a list of users logged on locally to a system.

1.14.3.2. The County has an unrestricted right of access to, and disclosure of, all information and software on any County equipment, or personal equipment used for County business or media, at the request of the appropriate County official(s). Information generated or placed into personally-owned personal computers being used on County time, as well as work undertaken on behalf of the County during or outside of any County worksite and/or work hours shall be made available for review at the request of appropriate County officials. For any applicable servicing, compliance auditing or forensics, this equipment shall be delivered to the County Information Technology facility or be made available through remote access. Such access and disclosure shall be in accordance with, and subject to any controls or restrictions imposed by applicable statutes or licenses.

1.15. WIRELESS SECURITY

1.15.1. Purpose

This section prohibits access to County networks by unsecured and unauthorized wireless communication mechanisms. Only wireless systems that meet the criteria of this policy, or that have been granted an exclusive waiver by the Director of Information Technology, are approved for connectivity to County networks.

1.15.2. Scope

This section covers all wireless information communication devices (e.g., personal computers, cellular phones, PDAs, tablet computers, etc.) connected to any County internal network. This includes any form of wireless communication device capable of transmitting information. Wireless devices and/or networks without connectivity to the County's networks do not fall under the purview of this policy.

1.15.3. Description

1.15.3.1. Wireless implementations shall:

1.15.3.1.1. Be pre-approved by the Information Technology Department.

1.15.3.1.2. Be compliant with the Information Technology Department's wireless architecture

1.15.3.1.3. Be managed by and within the Information Technology Department's wireless architecture.

1.15.3.1.4. Comply with all County Information Security Standards.

1.15.4. Devices using non-County wireless services (such as cell phone networks) shall not be used for information transmissions containing County protected information unless the connection is encrypted. Likewise, other broadcast networking technologies--such radio-based local area networks--shall not be used to transmit County protected information unless the link or the information itself is encrypted.

1.16. **PROTECTED INFORMATION**

1.16.1. **Purpose**

1.16.1.1. To establish policy for the handling, storage and destruction of protected County electronic information.

1.16.2. **Scope**

1.16.2.1. The information covered in this section includes, but is not limited to, information that is either stored or shared electronically by any means.

1.16.2.2. All employees shall familiarize themselves with the information labeling and handling principles that follow. The principle behind an information protection policy is that only the intended audience or authorized individuals should see or have an opportunity to see information and only authorized individuals should be able to modify information. Exceptions to this principle are made only by those who have the authority to do so.

1.16.2.3. For the purposes of this policy, all information is categorized into two main classifications:

1.16.2.3.1. Public information. Public information is defined as any information that can be made available to the public via the California Public Records act.

1.16.2.3.2. Protected information. Protected information is any information not declared by law or policy to be public information. Protected information includes the following, as defined by County policies and California and federal laws and regulations, as may be amended from time to time:

1.16.2.3.2.1. Personally Identifiable Information

1.16.2.3.2.2. Protected Health Information

1.16.2.3.2.3. Protected Criminal Justice Information

1.16.2.3.2.4. Protected Critical Infrastructure Information

1.16.2.3.2.5. Intellectual Property

1.16.3. **Description**

1.16.3.1. Protected Information

1.16.3.1.1. Protected information and media shall be suitably marked with the highest relevant sensitivity classification.

1.16.3.1.2. Access should only be granted to those individuals (County employees and affiliates) designated with approved access.

1.16.3.1.3. Electronic distribution within the County must be marked as "Confidential". Electronic distribution outside of the County must be encrypted securely.

1.16.3.1.4. Storage

1.16.3.1.4.1. Protected information shall be kept from view of unauthorized people. Access to work areas containing protected information shall be physically restricted. Visitor access to work areas containing protected information shall be controlled by guards, receptionists, or other staff.

1.16.3.1.4.2. Printers that are printing protected information shall not be left unattended until the protected printouts are removed.

1.16.3.1.4.3. Protected information should not be stored or displayed on machines without physical and software access controls.

1.16.3.1.4.4. All information storage media (such as hard disk drives, USB sticks, magnetic tapes, CD-ROMs, etc.) shall be encrypted and physically secured when not in use.

1.16.3.1.4.5. Any medium for backup/recovery shall have the same or better access and security controls as the original information.

1.16.3.1.4.6. Protected information shall not be stored in a given location any longer than the business function or law requires.

1.16.3.1.4.7. Protected information transferred to laptops, PDA's and all other portable media shall be encrypted. These laptops, PDA's and all other portable media shall remain in the possession of the traveler at all times (not be checked in).

1.16.3.1.4.8. Equipment that is no longer under the physical control of the County shall have protected information expunged/cleared prior to transferring control to an outside agency (e.g. surplus, sending equipment out for repair, loaning equipment, etc.). Alternatively, repair vendors shall execute a nondisclosure agreement with the County.

1.16.3.1.4.9. Individual access controls are required for protected electronic information.

1.16.3.1.4.10. Individual access controls for physical security are required for all forms of storage.

1.16.3.1.5. Disposal/Destruction:

1.16.3.1.5.1. Electronic information shall be expunged/cleared or zeroed.

1.16.3.1.5.2. Media shall be reliably electronically erased or physically destroyed.

1.16.3.2. The penalty for deliberate or inadvertent disclosure includes discipline, up to and including termination of employment and possible civil and/or criminal prosecution.

1.16.4. **Security Controls**

1.16.4.1. Information about security measures utilized for County computer and communication systems is confidential and shall not be released to anyone without written permission from the Director of Information Technology or the Chief Security and Privacy Officer.

1.16.4.2. As permitted by the California Public Records Act, the County shall not disclose information security records of a public agency if, on the facts of the particular case, disclosure of those records would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency.

1.16.5. **Encryption keys**

Encryption keys used for County information are classified as protected information. Access is limited to those who have responsibility for the management of those keys. Encryption keys shall not be revealed to consultants, contractors, temporaries, or third parties without the written approval of the Chief Security and Privacy Officer. Likewise, encryption keys shall always be encrypted when transmitted over any network.

1.16.6. **Encryption responsibilities**

1.16.6.1. When providing computer networking services, the County does not provide default message protection services such as encryption. Accordingly, no responsibility is assumed for the disclosure of information sent over the County's networks, and no assurances are made about the privacy of information handled by the County internal networks. In those instances where encryption or other special controls are required, it is the information owner's responsibility to make sure that adequate security precautions have been taken. However, nothing in this section should be construed to imply that County policy does not support the controls dictated by agreements with third parties (such as organizations which have entrusted the County with confidential information).

1.16.6.2. Whenever such facilities are commercially available, the County shall employ automated rather than manual encryption key management processes for the protection of information on County networks.

1.17. SECURITY INCIDENT RESPONSE

1.17.1. Purpose

1.17.1.1. The County will follow established policies and procedures to address indications that the security of the County's information technology resources may have been compromised. Such procedures include ensuring that the appropriate level of County management becomes involved in determining the response to an information technology security incident.

1.17.2. Description

1.17.2.1. Security Incident Definition

Security Incidents include, but are not limited to:

1.17.2.1.1. Actions apparently intended to harm or illegally access County information resources or information.

1.17.2.1.2. Potential violations of Federal law, State law, Business-specific Regulations or County Policy involving a County information technology resource or information.

1.17.2.1.3. A breach, attempted breach or other unauthorized access of a County information technology resource or information. The incident may originate from the County network or an outside entity.

1.17.2.1.4. Attempts (either failed or successful) to gain unauthorized access to a system or its information.

1.17.2.1.5. The infection of any County system with a worm, Trojan horse, rootkit, bot, crimeware, virus, ransomware, or other types of malware.

1.17.2.1.6. Conduct using, in whole or in part, a County information technology resource or information which could be construed as harassing, or in violation of County Policies.

1.17.2.1.7. Action or attempt to utilize, alter or degrade a County owned or operated information technology resource in a manner inconsistent with County policies.

1.17.2.1.8. Unwanted disruption or denial of service against County information technology resource or information.

1.17.2.1.9. The unauthorized use of an information technology resource or information.

1.17.2.1.10. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

1.17.3. **Security Incident Response Team**

The Chief Security and Privacy Officer shall maintain a Security Incident Response Team consisting of individuals from many disciplines, trained to respond to major security incidents. The members shall be equipped with the tools and understanding of security incident response processes and procedures, work through closed means of communication, and shall maintain confidentiality.

1.17.4. **Incident Reporting**

1.17.4.1. Employees and affiliates shall promptly notify the Departmental Information Security Officer when:

1.17.4.1.1. Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents have been perpetrated against the County

1.17.4.1.2. There is knowledge or a reasonable suspicion of an incident which violates the confidentiality, integrity, or availability of information.

1.17.4.1.3. A virus, worm, bot, rootkit, ransomware, or other malware has been discovered

1.17.4.1.4. It is unclear whether a situation should be considered a Security Incident

1.17.4.2. Departmental Information Security Officers shall notify the ITD Information Security Team of all but minor information security incidents.

1.17.4.3. Security Incidents involving possible violation of Federal or California law shall be reported to the County’s Chief Security and Privacy Officer.

1.17.4.4. Incident Reports shall include:

1.17.4.4.1. A description of events

1.17.4.4.2. Approximate timelines

1.17.4.4.3. Parties involved

1.17.4.4.4. Resolution of the incident (if any)

1.17.4.4.5. External notifications required

1.17.5. **Incident Escalation**

1.17.5.1. Upon notification of an incident, the County’s Chief Security and Privacy Officer or designee shall, as needed, escalate the incident to the County’s Security Incident Response Team.

1.17.5.2. If activated, the County's Security Incident Response Team shall plan and coordinate the activities of all departments involved, keeping other concerned departments advised. In carrying out this responsibility, the County's Security Incident Response Team shall ensure that operational decisions are elevated to the levels of County government required to protect the interests of the County and others impacted by the incident. Such decisions include, but are not limited to:

1.17.5.2.1. Restricting information system access or operations to protect against further information disclosure

1.17.5.2.2. Involving law enforcement agencies in cases where applicable statutes appear to have been violated

1.17.5.3. The Chief Security and Privacy Officer or designee shall document the deliberations, decisions, and actions of the County's Security Incident Response Team.

1.17.5.4. All external notification, reporting or publicizing shall be approved by the Department Head or the Director of Information Technology.

1.17.6. **Incident Actions**

1.17.6.1. If the incident appears to involve a compromised computer system, the state of the computer system shall not be altered. The computer system shall remain turned on, all currently running computer programs shall be left as is, and the computer shall not be used until directed otherwise by the County's Incident Response team.

1.17.6.2. Whenever system security has been compromised or if there is a convincing reason to believe that it has been compromised:

1.17.6.2.1. All passwords residing on the system or entered on the system shall be immediately changed by the person responsible for the account.

1.17.6.2.2. A trusted version of the operating system and all security-related software shall be reloaded from trusted storage media or original installation media.

1.17.6.2.3. All changes to user privileges taking effect since the time of suspected system compromise shall be immediately reviewed by the systems administrator for unauthorized modifications.

1.18. TERMINATION OF EMPLOYMENT

1.18.1. **Purpose**

1.18.1.1. This section identifies methods to effectively limit and remove access to information resources for both voluntary and involuntary terminations within the County organization.

1.18.2. **Scope**

1.18.2.1. This applies to all County employees and affiliates regardless of pay scale.

1.18.3. **Description**

1.18.3.1. **Voluntary separation/termination**

1.18.3.1.1. Since terminations can be expected regularly, utilizing an *Employee Separation/Termination Checklist* for outgoing or transferring employees, as part of standard HR "out-processing" ensures that system user accounts are removed in a timely manner. It normally includes:

1.18.3.1.1.1. Removal of access privileges, computer accounts, authentication tokens.

1.18.3.1.1.2. Control of keys.

1.18.3.1.1.3. Briefing on the continuing responsibility for confidentiality and privacy.

1.18.3.1.1.4. Return of property.

1.18.3.1.1.5. Verifying that files and information under the user's control are available or transferred to the department.

1.18.3.2. **Involuntary Termination**

1.18.3.2.1. In addition to the process identified for voluntary separation/termination, involuntary terminations shall include:

1.18.3.2.1.1. Terminating access as quickly as possible, preferably at the same time (or just before) the employee is notified of his/her dismissal.

1.18.3.2.1.2. If possible, during the "notice of termination" period, assign the individual to a restricted area to function, particularly where employees are capable of changing programs or modifying systems or applications.

1.18.3.2.1.3. Any time termination involves persons in a position of trust such as a systems administrator, the County shall have a replacement administrator chosen and ready to assume their duties as soon as possible.

1.18.3.3. **Termination Process**

1.18.3.3.1. In the event that an employee, consultant, or contractor is terminating his or her relationship with the County, the individual's immediate management is responsible for ensuring all property in the custody of the individual is returned, that the Information Technology Department is given prompt notification by utilization of a Termination/Separation Checklist in order to revoke all computer access rights for that individual, that administrators handling the computer accounts used by the individual are notified, and that all other work-related privileges of the employee are terminated.

1.18.3.3.2. Upon notification of an employee's termination from employment at the County, the following shall be accomplished:

1.18.3.3.2.1. The department manager or designee shall notify the Information Technology Department and complete a *Termination/Separation Checklist*.

1.18.3.3.2.2. The department manager or designee shall notify those departments in which the employee, consultant, or contractor had access through keys, tokens, or access cards so that access privileges can be deactivated.

1.18.3.3.2.3. Following the guidelines outlined in the checklist and the separation date, the Information Technology Department shall:

1.18.3.3.2.3.1. Ensure the individual's account(s) have been disabled.

1.18.3.3.2.3.2. Ensure the individual's access to standalone applications (those where access is not controlled by a central account) have been disabled.

1.18.3.3.2.3.3. Ensure the individual's name has been removed from any internal system access lists, authentication server lists, firewall lists, etc.

1.18.3.3.2.3.4. Change any network passwords the individual may have had access to (to include routers, firewalls, etc.).

1.18.3.3.2.3.5. Terminate the individual's access to unique County information technology resources. Change passwords if necessary.

1.18.3.3.2.3.6. Terminate remote access account(s) and access tokens (if applicable).

1.18.3.3.2.3.7. Assign access rights over the individual's files and directories.

1.18.3.3.2.3.8. Re-route email to the appropriate person identified by department management (if applicable).

1.18.3.3.2.3.9. When applicable, perform a general security scan of the system(s) for any unknown back doors, etc.

1.18.3.3.3. On or near the last day of employment or association with the County, the department manager or designee shall meet with the individual to receive identification materials, keys, tokens or access cards used to permit access to County networks and facilities. Access to non-public areas of facilities shall be cancelled upon termination of an employment relationship with the County and all physical security access codes known by the individual deactivated or changed.

1.18.3.3.4. In the event the individual has County equipment off-site, this equipment shall be turned over to the department manager or designee and forwarded to the Information Technology Department during the last scheduled day of employment or other association with the County.

1.18.3.3.5. The individual shall be asked to read and sign a non-disclosure agreement intended to protect confidential and private information.

1.18.3.3.6. Documentation of items received, and a copy of the termination/separation checklist shall be kept in the individual's permanent record of employment/association with the County.

1.18.3.3.7. All inactive user accounts shall be removed from County systems after a ninety (90) day period.

1.19. **EXCEPTIONS**

Under rare circumstances, the County may need to vary from these policies. All such instances shall be approved in writing and in advance by the Director of Information Technology and/or the Chief Security and Privacy Officer. Disputed issues may be escalated to the Information Technology Governance Committee for final decision as necessary.

1.20. **ENFORCEMENT**

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of services, and/or legal penalties, both criminal and civil.