SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

911

FROM: Riverside County Information Technology

SUBMITTAL DATE:
April 15, 2008

SUBJECT: Policy A-58 Enterprise Information Systems Security Update

RECOMMENDED MOTION: That the Board of Supervisors approve the attached additions to Policy A-58 Enterprise Information Systems Security, Sections 11 through 15.

BACKGROUND: On July 29, 2003, Agenda Item 3.39, the Board of Supervisors approved Policy A-58 Enterprise Information Systems Security Policy.

The purpose of the Enterprise Information Systems Security Policy is to guide the creation and maintenance of a secure information systems environment across all County departments, districts and agencies. Highlighted security features of this policy include: increased system security and availability, greater assurance of data integrity, additional protection of individual privacy, enhanced prevention of unauthorized access to information and information systems, and enhanced protection against misuse of, damage to, or loss of data. The Executive Technology Committee (ETC) has reviewed, commented, and is in consensus with the policy additions.

Continued on Page 2

Matthew W. Frymire
Chief Information Officer

FINANCIAL DATA				
	Current F.Y. Total Cost:	$ 0	**In Current Year Budget:**	N/A
	Current F.Y. Net County Cost:	$ 0	**Budget Adjustment:**	N/A
	Annual Net County Cost:	$ 0	**For Fiscal Year:**	N/A

SOURCE OF FUNDS:

Positions To Be Deleted Per A-30 ☐

Requires 4/5 Vote ☐

C.E.O. RECOMMENDATION:

APPROVE

BY: Elizabeth J. Olson

County Executive Office Signature

Departmental Concurrence

Dep't Recomm.: ☒ Policy ☐ Consent
Per Exec. Ofc.: ☒ Policy ☐ Consent

Prev. Agn. Ref.: 3.39, 7/29/03 | **District:** | **Agenda Number:** 3.22

Following is a summary of the proposed updates to the policy:

Section 11
An incorporation of ISO policy S05.01 Sensitive Data Protection, issued March 1, 2007. This policy provides departments guidance on what is sensitive data and how it should be handled and protected.

Section 12
An incorporation of ISO policy S03.01 Hardware and Software Controls, issued August 11, 2004. This policy gives the departments the authority to determine what hardware and software is acceptable to be used by their employees, within county standards.

Section 13
An incorporation of ISO policy S07.01 Archive Data Protection, issued November 29, 2006. This policy defines the proper handling of county backup media.

Section 14
An incorporation of ISO policy S01.01 Wireless Networking, issued May 1, 2006. This policy defines the wireless strategy in Riverside County.

Section 15
An incorporation of ISO policy S02.01 Analog Lines Management, issues April 12, 2004. This policy defines the departmental responsibility for requesting and maintaining analog lines.

Riverside County

Enterprise Information Systems Security Policy

Office of Primary Responsibility:
Chief Information Security Officer
County of Riverside
(909) 955-8282
Security@co.riverside.ca.us
http://www.co.riverside.ca.us

Board of Supervisors

Policy No. A-58

TABLE OF CONTENTS

1 General

1.1 Purpose

The purpose of this Enterprise Information Systems Security Policy is to guide the creation and maintenance of an environment across all County of Riverside departments (hereinafter referred to as "County") that:

- Provides for system security and availability;
- Assures data integrity;
- Protects individual privacy;
- Prevents unauthorized access to information and information systems; and
- Protects against the misuse of, damage to, or loss of data.

This policy shall serve as a foundation for the County's information security infrastructure.

The County shall attempt to manage information security in as unobtrusive a manner as is practical. The Chief Information Security Officer ("CISO") will work with each department to assist in the development of their specific security requirements, programs, processes, procedures and standards.

This is a County enterprise level policy, providing high-level policy and direction. Appropriate implementation standards, processes, and procedures with more detail must be developed by the County Executive Technology Committee ("ETC") and the individual departments to further define the implementation of this policy.

This policy is applicable to all information systems managed, owned, operated, maintained, or utilized by or on behalf of the County, and all users who utilize these systems. In addition, each non-County organization, which connects to or traverses the County Wide Area Network ("CORNET") shall develop their own internal standards, processes, and procedures that comply with this and other enterprise level policies.

For the purpose of this policy, the terms administrator, systems administrator, database administrator and department IT refer to the technical support staff responsible for the installation, maintenance, and administration of information systems, network hardware and software, as well as database administration and programming. As used in this policy, these terms do not imply specific job titles or pay grades associated with those staff positions.

Any exception to this policy shall be coordinated with and approved by the CISO.

Meet and confer issues and matters pertaining to discipline shall be coordinated with and approved by the Human Resources Director/Assistant CEO.

If there are conflicting requirements between this policy and other laws, regulations, or policies, the more stringent requirement will apply.

As used in this policy, "department" refers to all County departments, agencies and districts. All departments must comply with the requirements of this policy.

As used in this policy, "users" refers to all County employees, managers, contractors, and other personnel or persons who use or access County information systems. All County employees, managers, contractors, and other personnel or persons who use or access County information systems must comply with the requirements of this policy.

1.2 General Policy Statement

Information in any form, whether e-mail, data, voice, video, internet, microwave, or any other format, is a County entrusted asset requiring assurance commensurate with its value, criticality, and sensitivity. Measures must be taken to protect information from unauthorized use, modification, destruction, or disclosure, whether accidental or intentional, as well as to ensure its authenticity, integrity, and availability. Due care must be exercised to appropriately protect this information from origin to destination, both internal and external to the County information systems and networks.

1.3 Scope

For the purposes of this policy, security is defined as the ability to protect:

- The integrity, confidentiality, and availability of information processed, stored, or transmitted;
- Information technology assets from unauthorized use or modification; and
- All data and systems from accidental or intentional damage or destruction.

This includes but is not limited to the security of information technology facilities, off-site data storage, computing systems, telecommunications, applications and related services and Internet-related applications and connectivity, regardless of the location or personnel responsible.

1.4 Authority

This policy gives the Chief Information Security Officer ("CISO") and the Information Security Office ("ISO") in coordination with the Executive Technology Committee ("ETC"), and the Policy Advisory Committee ("PAC"), authorization for developing and maintaining security policies and systems to ensure the integrity of the County's information resources and to prevent the disclosure of confidential information. The CISO and ETC are also responsible for developing, approving, and implementing

standards for information technology, including but not limited to system design, architecture, integration, and interoperability.

1.5 Compliance

All users are responsible for complying with County security policies, standards, processes, and procedures. This includes building, configuring, operating, and maintaining networks and systems in accordance with these policies, standards, processes, and procedures. Anyone becoming aware of violations of this policy will immediately bring this to the attention of the CISO and the appropriate department authority. Any person who violates these policies, processes, or procedures may receive disciplinary action, up to and including termination. Any person who violates these policies, processes, or procedures may be subject to loss of network connectivity and criminal prosecution.

Outsourced services, processing and storage facilities (such as service bureaus, vendors, partnerships, and alliances) must be monitored and reviewed by the responsible department to ensure compliance with this policy. This will be accomplished through contractual commitments with provisions to permit auditing and monitoring to ensure compliance.

1.6 Deviations from Policy

Any deviation from this policy must be fully documented and a waiver granted, in writing, by the department head and the CISO. Any permitted deviations will be evaluated through the change control process and reviewed on an annual basis for continuation or revocation.

1.7 Document Changes and Feedback

This policy will be reviewed annually by the ETC and updated as necessary. Proposed changes will be submitted to the Board of Supervisors for approval. Meet and confer issues and matters pertaining to discipline shall be coordinated with and approved by the Human Resources Director/Assistant CEO.

1.8 Information Security Office

Under the leadership of the CISO, the Information Security Office (ISO) will develop and implement an enterprise security risk management program; publish enterprise security policies, standards, processes, and procedures; and provide programs and processes to facilitate the implementation of this policy.

2 Security Philosophy

2.1 Basic Principles

The basic security principles of the County are to protect the confidentiality, integrity, and availability of the County's information and information resources. The County is entrusted with these assets and owns the accountability for their protection.

- **Confidentiality** means that information deemed sensitive or confidential is protected such that it is unavailable to those who do not have the necessary approvals to access it.
- **Integrity** means that information is correct and has not been altered or corrupted in some way during transmission, processing, or while in secure storage. It also means that programs, applications, procedures, and systems function as intended.
- **Availability** means that access to information and information systems is not denied to authorized users.

Security is an enabler critical to the success of technology initiatives, and will not be viewed as a deterrent or irritant.

2.2 Functional Responsibilities

County enterprise security requires the active support and ongoing participation of all personnel involved. It requires management support and universal compliance. Responsibility for satisfying requirements is shared and extends to all personnel involved with the development, implementation, operations, use, and maintenance of County information systems.

2.3 Information Assurance

Information security encompasses many disciplines, including computer security, network security, communications security, and physical security. For County systems, security will be based upon the concept of information assurance. The overall goal of information assurance is to protect and defend information and information systems. Disruptions are not preventable 100% of the time; therefore, the County must be prepared to respond appropriately and recover to ensure the confidentiality, integrity, and availability of the information and information systems. Information assurance includes information protection, event detection, restoration of information and services, and appropriate response. The County must protect information and information resources from intentional, unintentional, structural, and environmental threats; detect threats and attacks; restore capabilities in an efficient and prioritized manner; and respond appropriately with an integrated, coordinated, and focused effort to cope with, reduce, or eliminate the effects of attacks or intrusions.

2.4 Defense-In-Depth

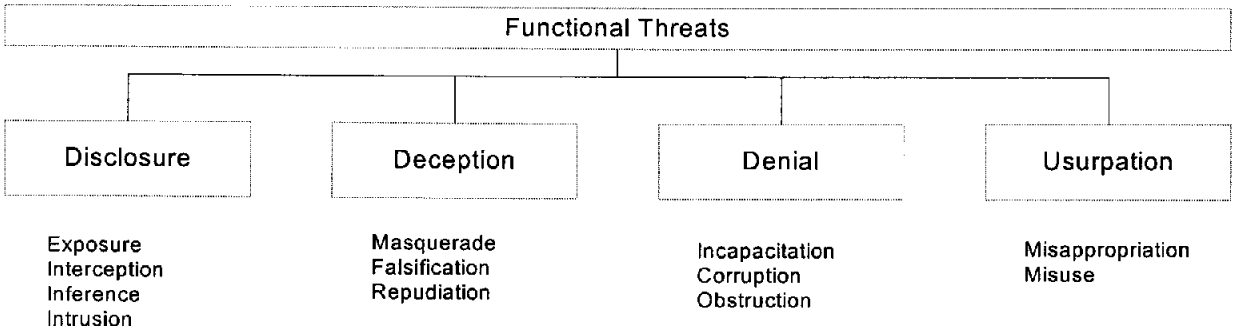
The County's servers, workstation computers, networks, network components, and other information technology devices shall be implemented within a defense-in-depth framework. Defense-in-depth is a multi-faceted security approach that includes both technical and non-technical layers of security to protect resources. Defensive countermeasures are used to reinforce each other, protecting information and resources while allowing response activities to be undertaken quickly and efficiently. No single security technique or mechanism is solely relied upon to protect valuable resources, resulting in a higher degree of security.

The reasons for this approach are fundamental. No network or system can be completely secure, as it is impossible to identify all possible vulnerabilities and apply the appropriate countermeasures. Taking this reality into account, security and detection should be implemented in layers such that a hole in one layer will be covered by other layers. This approach, in combination with an information assurance strategy, provides the best opportunity to reduce risks to acceptable levels.

2.5 Threats

County information resources are vulnerable to many threats. These threats can inflict various types of damage, ranging from errors that harm databases to fires that destroy entire computer centers. Some threats affect the confidentiality or integrity of data while others affect the availability of a system. The potential impact of all threats will be considered when conducting a risk assessment, no matter how ad-hoc or informal the assessment. While considering threats, the fact that threat assessments are inherently inaccurate and incomplete must be taken into account.

Threats can be categorized both by source and function. The following threats are representative and not intended to be all-encompassing:



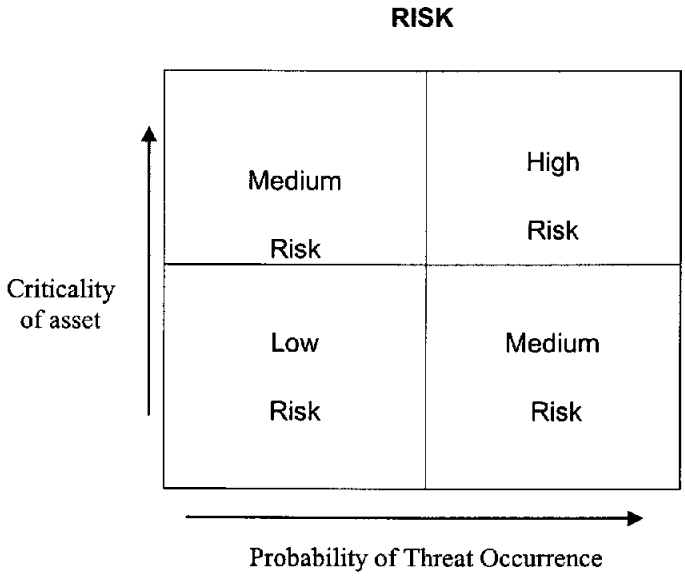
2.6 Risk Management

It is impossible to eliminate all risk; therefore, security exists to mitigate risk to acceptable levels. All security decisions will be made with risk management in mind. An assessment must be made to determine what can be done to reduce risk to an acceptable level under the circumstances. Risk-based decisions must be made keeping in mind the vulnerability and criticality of the assets. If reliable, up-to-date threat information is available, it will be considered but not serve as the major basis for risk management decisions because there are wide unknowns inherent in threat assessments.

Risk management can be broken down into four basic questions that can be applied to virtually any situation:

1. What can hurt me?
2. How can it hurt me?
3. How critical is this?
4. What can I do to protect myself?

The following graphical representation portrays risk as a quad chart:



2.7 Access Control

To facilitate the development of a defense-in-depth security strategy, including restricting physical access to resources and logical access to computers and networks, it is imperative that all security systems which make access control decisions based on identity of an individual be linked together. It is crucial that all

security systems are linked in such a manner that there is an employee identity clearinghouse and public key infrastructure linked together through a meta directory developed to form this wide area network. In this manner, all access control policies directly related to the wide area network may be orchestrated at a single point and be integrated with existing and future technologies such as enterprise resource planning systems.

Access control decisions are to be made based on the concept of least privilege, in which individuals are given access based on job duties and responsibilities. The concept of least privilege dictates that individuals are given only those accesses and rights necessary for job completion, and no more. The results of all access decisions are to be logged and retained by the department.

2.8 Enterprise Information Assurance

To meet existing and new security challenges, the County shall implement an enterprise-wide information assurance architecture following a secure framework. County computer systems and networks are increasingly interconnected. Because of that fact, in many cases a risk accepted by one County department is a risk imposed upon others. Therefore, an enterprise approach to security is required that enforces common security policies, standards, processes, and procedures. Security must be considered end-to-end; that is, from the point of origin to the point of delivery. Security systems must migrate towards utilizing common directories or meta-directory containing a single record for each individual with associated access control policies. This structure will facilitate management of accounts and access at the department level; and will also provide for common policies and procedures and consistent decision points.

3 User Requirements

3.1 Identification and Authentication

Access to all County systems located behind County firewalls requires robust, continuous, and reliable authentication.

3.2 Passwords Management Policy

Passwords must be strong and well guarded. The department IT administrator for each environment will approve all new accounts. New accounts will be set up in accordance with this policy and any applicable department requirements. Users are responsible for choosing passwords that are highly secure. Users shall never divulge their passwords to others, even their superiors, fellow employees or IT administrators.

The following is a list of rules for creating strong passwords:

- Contain one number, capital letter, or special character.

- Be at least 8 characters in length.
- Be changed at least every 90 days.
- Never be the same as the user's logon ID.
- Not contain the user's phone number (wholly or partially).
- Not be common words or phrases.
- Not be a name such as wife, husband, child, or pet.
- Not be a word found in the dictionary.
- Not be changed more frequently than once a day.
- Not be reused within the last five password changes.

3.3 Unattended Computers

Users will either log off or lock the system when they will be away from the computer for any length of time. (Recommend no more than 15 minutes without log off or lock.)

3.4 Software Import Control

Each modification runs the risk of introducing viruses, damaging the configuration of the computer, or violating software-licensing agreements. The County must reduce the risk of introducing malicious code into the County network.

County departments will maintain approved software application lists for their systems. The department IT administrator will approve all software before it can be added to the listing, or installed on a County computer. Software will be installed only from approved sources to limit exposure to contaminated software. No software will be downloaded from any Internet location without prior written approval from the departmental IT authority.

3.5 Viruses

Viruses can cause serious damage. The County must prevent the release of viruses on the County network.

3.5.1 Prevention

Department IT administrators will install anti-virus software approved by the DTSC on all file and mail servers to limit the spread of viruses within the network. Workstations will have memory resident anti-virus software installed and configured to scan data as it enters the computer. Programs will not be executed, nor files opened by applications prone to macro viruses, without prior scanning for viruses.

All incoming mail and files received from across a network must be scanned for viruses as they are received and prior to delivery to email boxes. Virus checking will be performed, where applicable, at firewalls and gateway SMTP servers that control access to networks. This allows for centralized virus scanning for an entire department.

Virus scanning definitions shall be updated at least on a weekly basis to remain current with the latest viruses. It is important for employees to immediately inform their IT administrator of any different or out of the ordinary behavior which a computer or application exhibits. The IT administrator shall immediately disconnect a computer that is infected or thought to be infected from networks to reduce the risk of spreading a virus.

3.5.2 Detection

All software must be installed on a test bed and scanned for viruses before being allowed on an operational or production machine. Only after receiving approval through the departmental change management process may software be moved to production systems. Use of off-the-shelf scanning software will be enhanced by state of the art virtual machine emulation for polymorphic virus detection. All other new virus detection methods will be incorporated into the detection test bed. Scanning software will be updated weekly or more often if updates are available.

Virus scanning of all file servers on a weekly basis is mandatory. All data imported onto a computer from any source (such as floppy disk, e-mail, or file transfer) will be scanned before being opened, executed or used.

Department IT administrators will immediately advise the Department of Information Technology Network Control Center ("NCC") when a virus is launched. The NCC will then inform the CoNSERT members and all other departments that may have access to the same programs or data that a virus may have infected their system.

3.6 Interactive Software

Use of unapproved interactive software is prohibited. The department IT authority is responsible for approval of all such software. Web browsers, and where applicable, firewalls, will be configured and the configurations audited by the department IT staff to inhibit the downloading of unauthenticated or unauthorized applets. Browsers will be configured to prohibit un-trusted Java scripts or Active X from running automatically.

3.7 Software Licensing

Employees shall use software only in compliance with license agreements. Software will not be downloaded over the Internet without prior approval of the department IT administrator. All software used on County computers must be approved by the department IT administrator, and will comply with all licensing requirements and procedures. The department's IT staff will inspect computers periodically to verify that only approved and licensed software has been installed. On an annual basis, all software used on all departmental systems must be reported to the Riverside County Information Technologyas part of the County software license compliance audit.

3.8 Encryption

Encryption shall be used for sensitive or confidential data that will be stored in non-secure locations or transmitted over open networks (such as the Internet). Encryption of any other County information must be approved in writing by the department head. Where encryption is used, County- approved standard algorithms and standard products must be used. The minimal encryption key length for sensitive or confidential data is 128 bits or greater.

The use of a random number generator is recommended for generating keys for encryption of County information. Encryption keys will be considered sensitive information and access to those keys must be restricted on a need to know basis.

When encryption is used, secure means must be used for all distribution of secret keys. Acceptable approaches include:

- Use of public key exchange algorithms.
- Double wrapped internal mail.
- Double wrapped courier mail.

Encryption keys must not be sent via e-mail, unless the e-mail is encrypted using keys that have been previously exchanged using secure means.

All encryption products used must support some form of technology to make data available to County management. Where encryption is used, County-approved key recovery implementations must be used.

3.9 System Architecture

System architectural vulnerabilities impact overall system security. Initial consideration for system architecture shall be the configuration of the firewalls and the connections to the Internet. Other areas that require security consideration include: use of the Internet to connect physically separate networks, Virtual Private Networks ("VPN"), and remote access to internal systems, email, and databases from the Internet.

3.10 Remote Access

All remote access to computer systems on CORNET, whether via dial-up or Internet access, must use encryption services to protect the confidentiality of the session.

Remote access for systems administration purposes to computer systems, network devices, and/or firewalls attached to CORNET will only be permitted through VPN or remote dial-in solutions approved by the DTSC and CISO. This applies to any user who has been granted this type of access.

Information regarding access to County systems, such as dial-up modem phone numbers or VPN IP addresses, is considered confidential. This information must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or made available to third parties without the written concurrence of the CISO and the department IT administrator.

The CISO will periodically scan direct dial-in lines to monitor compliance; and may periodically direct the department to institute a change of telephone numbers to make it more difficult for unauthorized parties to locate County communications numbers.

3.10.1 Virtual Private Networks

When the Internet is used to provide VPN connections between sites, a means of rapidly providing backup connections must be maintained to return service in the event of an Internet outage or denial of service. All VPN access points will be approved by the CISO as part of the security architecture framework. Existing VPNs will undergo a security assessment; and be brought into compliance with standards and approved by the CISO or disabled within 12 months of the approval and publication of the DTSC VPN standard.

The establishment of VPNs over the Internet between County networks requires prior approval of the CISO. Adding networks to an existing VPN also requires prior approval of the CISO. A review and update of the security policies in use at each site to be connected to the VPN must be performed by the CISO before operation will be authorized.

3.10.2 Dial-In Access

All users who access County systems through dial-in connections must use only approved dial-up connections to ensure the integrity of the session. Direct dial-in connections to County production systems must be approved by the department IT administrator and the CISO. All shared/common dial-up access points will be managed and maintained by the Department of Riverside County Information Technology as part of the security architecture implementation of CORNET. Remote access dial-up servers which do not comply with these requirements are prohibited. The installation and/or use of desktop modems to support dial-in access to County systems is prohibited.

3.11 Internal Database Access

Access to internal databases by sources outside CORNET must use a County approved web interface portal. This web portal will be located in a certified Virtual Data Center or DMZ and will be required to meet all County security guidelines. Any County sensitive or confidential data to be stored on an external server shall be afforded the appropriate levels of protection.

3.12 Firewalls

All border firewalls will be periodically reviewed and their configurations approved by the CISO. The department IT administrator will inform the CISO in advance of all proposed changes to their firewalls. The CISO must approve in advance all changes to any border firewall within the architecture framework.

Where multiple firewalls are used in parallel for availability (fail-over configuration) or performance reasons, the configuration of each firewall shall be identical and under the control of a single firewall administrator.

Any sensitive or confidential data made accessible on internal networks that are connected to the Internet must be configured in a Transaction Zone (DMZ) and protected by a County-approved firewall. Each DMZ environment will be certified by the CISO. Periodic audits will be done by the CISO to ensure continued compliance with certification standards. If at anytime a DMZ fails to meet these requirements it will be shut down at the direction of CISO. Firewalls shall be configured to restrict access to such data to only authorized users.

3.13 Intrusion Detection

Intrusion detection plays an important role in implementing a security policy. An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusions can be categorized into two main classes:

- Misuse intrusions are well defined attacks on known weak points of a system. They can be detected by watching for certain actions being performed on certain objects.
- Anomaly intrusions are based on observations of deviations from normal system usage patterns. They are detected by building up a profile of the system being monitored, and detecting significant deviations from this profile.

3.13.1 Function

Intrusion detection provides two important functions in protecting information system resources. The first is that of a feedback mechanism which informs the security staff as to the effectiveness of other components of the security system. (The lack of detected intrusions is an indication that the perimeter defenses are working.) The second function is to provide a trigger or gating mechanism that determines when to activate planned responses to an incident.

3.13.2 Implementation

Normal logging processes shall be enabled on all host and server systems. Alarm and alert functions, as well as logging, of any firewalls and other network perimeter access

control systems shall be enabled. All critical servers should have additional monitoring tools which provide appropriate software wrappers, as a supplement to the activity logging process provided by the operating system. At logical network concentration points, intrusion detection system tools shall be installed which monitor for traffic patterns consistent with known attacks.

3.14 Administration

System integrity checks of the firewalls and other network perimeter access control systems shall be performed by the department IT administrators on a routine basis. Audit logs from the perimeter access control systems should be reviewed daily. Audit logs for servers and hosts on the internal protected network shall be reviewed on a regular basis by the department IT administrators.

All trouble reports received by department IT staff shall be reviewed for symptoms that might indicate intrusive activity. Suspicious symptoms will be immediately reported to the department IT administrator, who will then inform the CISO.

Host based intrusion tools shall be checked on a daily basis by the department IT staff. Network traffic monitoring intrusion detection systems will be checked by the CISO on a periodic basis for proper function and configuration.

The CISO will form an Intrusion Response Team (IRT) for the County. The IRT and network security personnel will establish relationships with other incident response teams and share relevant threats, vulnerabilities, or incidents.

The County will attempt to prosecute intruders, but will not allow security holes to go uncorrected in order to learn more about the intruder unless approved in advance in writing by the data owner.

3.15 Assigning Responsibility

Department IT administrators, in coordination with the CISO, are responsible for implementing information systems security related to County Intranet and Internet access. Roles and responsibilities shall be coordinated between administrators. If a department is attacked, it may be necessary for other departments to take action.

A personnel screening process shall be in place for critical functions/roles. Such personnel must satisfactorily complete the screening before being giving administrative privileges beyond local PC administrative privileges. Critical functions/roles are defined as system, network, DBA, LAN, and WAN administrators, security personnel, and other sensitive positions deemed critical by department management.

System, network, DBA, LAN, and WAN administrators, as well as other privileged roles, shall be given incremental access. More privileges will be granted only as the extent of their job function and level of trust increases.

Managers of critical functions/roles are responsible for determining job function and scope so that broad system and network privileges are not excessively granted. Local administrative privileges on County computers will only be granted to individuals where a business need justifies the required privilege. Department management is responsible for documenting and approving privileges, and ensuring the Administrator Agreement (Appendix C) has been executed and is kept in the department's file.

The department IT administrator, with permission from either the department head or the CISO, may temporarily suspend access privileges of any user if deemed necessary to maintain the integrity of any computer system or network.

4 Department, Agency and District Requirements

4.1 Operation

Each department must operate in a manner consistent with the maintenance of a shared, trusted County environment for the protection and assurance of data and transactions. Each department shall not jeopardize the confidentiality, integrity, or availability of the County enterprise, or the information stored, processed, and transmitted by County information systems.

4.2 Access Control

Stringent processes must be in place within each department to ensure only authorized personnel are granted and retain access to any information system. Department heads are responsible for ensuring that their IT administrators are provided verifiable authorization for the creation of and termination of accounts. Accounts shall not be left active after termination or contract completion. Each department will establish a policy to provide a stringent means of access control and periodic review of active accounts to minimize the risks associated with unnecessary accounts.

4.3 Termination Process

Each department will ensure that tested processes are in place for the immediate termination of access when users are terminated. This should cover as a minimum: account and permission termination; server and resource password changes; physical credential return; and return of equipment or other County property. These processes shall be complete and thorough to include but not be limited to network access, remote access, VPN, email, network devices, or other information system access.

4.4 Compliance

Each department is required to follow County security policies, standards, processes, and procedures.

4.5 Local Policies, Procedures and Standards

Each department will develop, implement, and maintain security policies, standards, processes, and procedures in accordance with this policy and as outlined in Appendix A.

4.6 Personnel Awareness and Training

Each department will implement a security awareness, training, and education program to ensure its staff is appropriately trained in the information security procedures. Each department must make all staff aware of the need for information security, and provide suitable training to ensure that personnel are prepared to perform the security procedures for which they are responsible.

4.7 Review Requirements

Each department will review and update its information security policies, standards, processes, and procedures at least annually; and also after any significant change to its business, computing, or telecommunications environment. Each department shall provide a report to the CISO documenting each review. The report will identify necessary changes and any discrepancies with County policies, standards, processes, or procedures.

4.8 Security Audits

Each department will have a security compliance audit performed every two years. Once each five years, a third party will perform the audit. In addition to these audits, the CISO will work with the County Auditor to audit separately, information technology security processes, procedures, practices, and compliance with this policy.

4.9 Vulnerability Assessment

Each department will have a vulnerability assessment performed on their information systems every two years by a third party. The third party shall prepare a written report of its findings. The findings will be submitted to the department head, and to the CISO. The CISO will work with the department as needed to assure compliance with this policy. After a period of one year from the implementation of this policy, the ISO may conduct random unannounced assessments of department systems to assess their security and response levels.

4.10 Risk Assessment

Each department will perform an annual risk assessment of their information systems. This assessment shall be used to identify, prioritize, plan for, and implement additional security measures. The assessment methodology shall be developed by the CISO. The CISO shall provide assessment training to appropriate personnel.

4.11 Life Cycle Management

Security requirements shall be defined and addressed by the department throughout the life cycle of the system or application.

4.12 Certification and Accreditation

Each County information system must complete a certification and accreditation process prior to being placed in production. Current systems will have 18 months to retroactively go through the process, once the process has been established and training has been provided. Thereafter, each information system shall be re-certified at least every three years and also after significant system changes which may invalidate the certification.

4.13 Conflicts in Policy

All departments shall comply with all applicable federal and state laws and regulations. Where there are any conflicts between applicable requirements, then the more stringent requirement will apply.

4.14 Privacy

Individual privacy will be protected as required by law.

4.15 Monitoring

Monitoring of information system usage will be conducted by the ISO in conjunction with Riverside County Information Technology (RCIT). Each department will also monitor their own systems as appropriate. Use of County systems implies consent to such monitoring by users.

4.16 Architecture and Modifications

Network architectures shall be formally documented by each department with such information provided to the CISO, including but not limited to equipment, functionality, and IP addresses. Updates are to be provided to the CISO as changes occur.

Each department shall process network changes affecting enterprise network traffic through the change control process, and provide written reports of proposed and approved changes to the CISO.

4.17 Incident Reporting

Each department shall develop procedures for reporting all security incidents. This will include notification to the ISO.

4.18 Environmental

Computer resources will be protected against structural and environmental threats, including appropriate cooling and humidity control and fire suppression.

4.19 Physical Protection

Computer resources and physical information, including but not limited to servers, desktops, laptops, network equipment, firewalls, hard copies, and tapes, must have appropriate physical protections in place.

4.20 Protection Profiles

System profiles shall be provided to the CISO to facilitate alert and response mechanisms. These profiles shall be provided and maintained according to processes established by the CISO. All system vulnerabilities shall be assessed by the department with a determination made on appropriate countermeasures to implement.

5 Internet Access and Email

5.1 Board Policy A-50

Use of County Internet and email systems are subject to the requirements of County of Riverside Board of Supervisors Policy A-50. Users must use the County Internet and email systems in accordance with Policy A-50.

5.2 Internet Access

In general, the County is fully interconnected with the Internet and other networks. However, the County may use software tools to block or limit access to certain Internet sites or networks. The ability to access an Internet site or network from a County system does not mean that use of that Internet site or network is proper or authorized.

Users who post to Internet sites (such as newsgroups, Internet mailing lists, or similar sites) through County systems shall not misrepresent their capacity or authority to do so.

Access to and use of County Internet systems or other networks from a non-County location must comply with this policy. Users shall not allow family members or non-authorized users to use County Internet systems or other networks.

5.3 Consent to Monitoring

The County has the ability to monitor the use of any County systems, including the Internet and email systems; and the County reserves the right to do so for any proper

County purpose (including but not limited to appropriate recording and auditing). The use of such systems is consent by users to such monitoring.

6 Written Acknowledgment

Department heads shall have all users acknowledge in writing that they have received, read, and understand this policy. The responsible manager shall also sign this written acknowledgement as the approval authority for granting the user access to County systems. Such written acknowledgment shall be retained in department files.

User Agreement (Appendix B): This must be signed by all users prior to granting access to County systems.

Administrator Agreement (Appendix C): This must be signed by all administrators prior to granting administrator access to County systems. Administrators must also sign the User Agreement.

Remote Access Agreement (Appendix D): This must be signed by all remote access users prior to granting remote access service ("RAS") or virtual private network ("VPN") access to County systems. Remote access users must also sign the User Agreement.

7 Logon Notice

A logon notice and warning banner shall be utilized on all County systems. This serves to remind users of County policies and to warn intruders of monitoring and unauthorized or illegal use. At a minimum, the logon notice shall include the following text:

"This is a County of Riverside system and is to be used only by County-authorized users in accordance with applicable laws and County policies, rules or procedures. This also applies to internet use and to all related or connected systems, networks, devices, and equipment.

County systems may be monitored by the County in accordance with County policies, rules or procedures, or as allowed by law. Any information placed on or sent through this or any other system may be subject to such monitoring. Use of County systems constitutes consent to such monitoring.

Authorized users shall not use County systems in an improper or unauthorized manner."

8 Configuration Control/Change Management

A configuration control and change management policy shall be created by the DTSC to facilitate the introduction of changes or modifications to County networks or

systems. Each department will define and document configuration control and change management procedures for systems under their control. The CISO will review and approve these procedures.

9 Security Education

It is the policy of the County to provide periodic security awareness training to all users. Such training will address the new and rapidly changing issues regarding security and the Internet. Department IT staff are encouraged to scan security-related lists, keep up with security and technology issues, and share security relevant information with the CISO and other CoNSeRT members.

New users shall receive an orientation to this policy and County security considerations. All users shall sign the User Agreement (Appendix B).

Users shall also receive continuous security training in the form of news flashes, security alerts or tips via the system, memos, computer incident alerts, and other appropriate training as determined by the department.

10 Engineering and Developers

Engineering and development systems shall be segmented into a DMZ away from the trusted portion of CORNET. Engineering and development systems are subject to separate configuration control and change management procedures developed by the department and approved by the DTSC and CISO. These procedures must be fully documented to ensure consistency of enforcement and implementation.

Application developers must develop secure applications consistent with established policies, standards, processes, and procedures. Applications shall protect individual privacy, confidentiality of electronic commerce information, and the integrity of both the application and the information it processes. Applications must log significant security events, protect the log files appropriately, and prevent co-mingling of data. Because of the nature of this work, development will be done on a network segment separate from the County trusted network. Suitable protections, access control restrictions, and firewalls will be put in place to ensure that development systems do not introduce vulnerabilities to CORNET.

11 Sensitive Data Protection

This section establishes countywide rules for the protection of Riverside County information and information assets. County departments are required to define how information is to be classified based upon its relative sensitivity and to help employees determine under what conditions information may be disclosed to non-employees. This establishes policy for the protection of sensitive information and data

Any user who is authorized to access Riverside County's information has an obligation to safeguard and protect the confidentiality of such data. The objective of this policy is to minimize the likelihood that sensitive or confidential County information is inadvertently disclosed.

11.1 Information Classification

Information ownership is the direct responsibility of user departments. Department heads and/or designees are responsible for being knowledgeable about confidentiality and privacy laws specific to their Department's functions. Department Heads and/or designees are responsible for all aspects of the classification, use, distribution and protection of County information within and outside of their respective departments. This responsibility includes determining the level of access granted to each user. Information owners are responsible for coordinating with their information custodians to assure that facility security needs of sensitive information are met.

Each department or agency is required to document public versus sensitive data under it's control. Questions about the proper classification of a specific piece of information will be addressed to the Information Owner. The Information Owner is the Department Head responsible for the information or information system. The Information Owner is the classification authority. It is the responsibility of the information custodian to apply appropriate measures to protect all information assets that are classified as sensitive by the owner of that information.

11.1.1 Guidelines

All information is categorized into two main classifications:

- Public
- Sensitive

11.1.1.1 Public Information

"Public information" is information that is available to anyone who asks based on legislative mandate, such as County, state, and/or federal regulations or declared to be public by someone within the County, with the authority to do so. This information will be provided via due process in order to ensure that the information is in fact public and that the cost for providing the information is appropriately recovered.

This is information that has been declared public under the California Public Records Act. For guidance on releasing public information beyond the scope of one's immediately defined work responsibilities, refer to your Information Owner or County Counsel. For more information, see the California Public Records Act contained within California Government Code 6254.9.

Unless regulations demand otherwise, any information that is marked "Draft," "Confidential," or "Sensitive" is not public by definition. If information is not marked or otherwise classified, County information is presumed to be sensitive unless expressly determined to be public information by the Information Owner or designee.

11.1.1.2 Sensitive Information

Sensitive information can be broken down into other classifications: restricted, private or confidential, protected, and intellectual property. Sensitive information includes personal, medical records or financial information on employees, constituents, citizens, customers, business partners, or anyone else that has not been previously defined in law to be a public record. Sensitive information may also include any other information that could enable an individual to commit identity theft when so defined in law or policy. Other sensitive information includes critical infrastructure schematics or infrastructure protection plans, including buildings, vehicles, telecommunication, and systems. Information, which is covered by non-disclosure agreements or intellectual property practices, is considered sensitive information.

11.1.1.2.1 Restricted Data

Information of this nature is sensitive and could have immediate detrimental effects if released to the wrong individuals. Specifically, restricted information could expose individuals to danger, suspend large segments of business operations, or cause extensive damage to resources. Examples of restricted information include California Law Enforcement Telecommunications System (CLETS), Coroner, District Attorney, and Public Defender, system documentation, and details about the operating environment hosting restricted information.

11.1.1.2.2 Private or Confidential Data

Some data collected and maintained by the County are protected from public disclosure through various privacy and confidentiality statutes, and thus are not available under existing public information laws. Examples of private or confidential information include:

- Passwords
- Social Security Numbers (SSN)
- Personal or family information
- Family names
- Age
- Personal or business partner financial and banking data, including credit cards, bank routing numbers and bank account information

- Personal information provided by constituents in the course of delivering any public health or social service (name, address, phone, SSN, family names, personal historical detail)
- County financial data not deemed public by the Public Records Act
- Employee performance reviews, discipline reports and other personnel data
- Information related to in-progress legal proceedings
- The combination of a logical address, User ID, and password
- County-owned or third-party Intellectual Property
- HIPAA data (Protected Health Information- PHI)

11.1.1.2.3 Protected Data

Protected data is information generated in the normal course of managing County operations and may be a public record under the State of California Public Records Act; however, if made available by publishing in a public medium the information would create a potential physical threat or potential disruption to County operations.

Examples of protected information include:

- Telecommunications and cabling schematics
- Disaster Recovery Plans
- Operational Recovery Plans
- Network schematics
- Physical facility schematics
- Preliminary reorganization plans
- Detailed information about ongoing projects
- Time sensitive information
- Risk assessments
- System controls and logs

11.1.1.2.4 Intellectual Property

Without specific written exceptions, all programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the County are the property of the County. When the County has legal ownership it therefore maintains exclusive rights to patents, copyrights, inventions, or other intellectual property developed by employees, consultants, or contractors for use on County systems. This includes intellectual property stored on County computer and

network systems as well as all messages transmitted via these systems. County software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-County party for any purposes other than official County business.

Registered software purchased from a non-County source is considered third-party intellectual property. Ownership and limitations on use are established by the registered owners' licensing agreements.

11.1.1.3 Declassifying or Reclassifying Information

Only the Information Owner may downgrade or declassify information. Downgrading is the process, as an example, of reclassifying information from "Restricted" to "Confidential."

11.1.2 Data Protection Guidelines

The sensitivity guidelines in this section provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as County information in each column may necessitate more or less stringent measures of protection, depending upon the circumstances and the nature of the County information in question. A given sensitivity designation is assumed to stay in effect until explicitly changed by the Information Owner or designee.

11.1.2.1 Minimum Information Protection

For use with general organization information; personnel information; and general technical types of information.

Labeling

Marking or labeling is at the discretion of the owner or custodian of the information. If marking is desired and the information is not Public, the words "County <Department Name> Sensitive" may be written or designated in a conspicuous place on or in the information in question. Electronic files may be labeled in the category field under the "File-Properties-Summary" tab. Other labels may be used at the discretion of the individual business unit or department.

Access

- Access should be provided to County employees and non-employees with a business need to know.
- All data including Public information requires access controls for authorized changes

Distribution within County is authorized through:

- Standard interoffice mail
- Approved electronic mail
- Electronic file transmission methods

Distribution outside of the County is authorized through:

- U.S. mail and other approved carriers
- Electronic distribution sent to approved recipients

Storage

- Keep information from view of unauthorized people
- Information should not be stored or displayed on machines without physical and software access controls
- Protect information from loss
- Any medium for backup/recovery should have the same or better access and security controls as the original data
- Electronic information should be protected with file properties to set individual access controls where possible and appropriate
- Information should not be stored in a given location any longer than the business function or regulation requires (e.g., downloading files to telecommuting machines, laptops, personal device assistants etc.).
- Equipment that is no longer under the physical control of the County must have information expunged/cleared prior to transferring control to an outside agency (e.g. surplused, sending equipment out for repair, loaning equipment, etc.).

11.1.2.2 Protection For More Sensitive Information

Information that is more sensitive includes Private or Confidential Data, Protected Data and Intellectual Property data. In addition to the above conditions, the following applies to information that is more sensitive:

Labeling

- Marking must indicate "Sensitive"

Access

- A signed nondisclosure agreement shall exist

Electronic distribution for all destinations

- Transmission must be via a private link or securely encrypted

Storage

- Information transferred to any portable media must be encrypted

11.1.2.3 Protection For The Most Sensitive Information

Information that is most sensitive includes Restricted Data. In addition to the criteria specified in the previous protection levels, the following applies to most sensitive information:

Labeling

- Marking must indicate "Restricted"

Distribution within the County

- Delivered direct — signature required, envelopes stamped classified

Distribution outside of the County internal mail

- Delivered direct, signature required
- Approved carriers
- Electronic transmission must be securely encrypted

Storage

- Individual access controls are required for all forms of storage

11.2 Mobile Devices or Portable Media

Storage of sensitive information on mobile devices or portable media is permitted only if all of the following requirements have been satisfied:

- Use is restricted to individuals whose official duties require it;
- Use is granted for a finite duration, as needed to fulfill the specific functions required to perform a specific job;
- The employee has obtained approval from both their department head and the Information Owner. For non-County employees, "department" is defined as the County department or agency contracting with the 3rd party;

- Sensitive data is encrypted. Encryption must comply with approved County standards.

Mobile Devices include:

- Any mobile device (County-owned or privately owned) capable of storing data.
- Examples include, but are not limited to, laptop, tablet PCs, Blackberries, cell phones, personal device assistants (PDAs), universal serial bus USB (thumb) memory data storage drives, external storage devices, iPods and MP3 players.
- For the purpose of this policy, all non-County-owned computing or data storage equipment, such as, personal computers (PCs), servers, Network-Attached Storage (NAS), Storage Area Network (SAN) are considered mobile devices. The department or agency must explicitly authorize use of such equipment within their environments.

Portable media includes:

- Any portable media (County-owned or privately owned) capable of storing data.
- Examples include, but are not limited to, external hard drives, USB thumb drives, flash drives, memory sticks and cards, Compact Disc (CDs), Digital Video Disc (DVDs), floppy disks.

11.3 Reporting Lost Data

In the event that County sensitive information (including that stored on a mobile device or portable media - encrypted or unencrypted) is lost or stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, it must be reported immediately to the appropriate department or agency management designated by Department policy and the ISO.

12 Hardware and Software Control

To prevent the introduction of malicious code and protect the confidentiality, integrity, and availability of County information resources, all hardware and software shall be obtained from or authorized by the department head or their designated agent. This includes equipment such as servers, PCs, laptops, printers, cell phones, radios, PDAs, telephones, portable media such as USB drives, compact disk – read only memory (CD-ROMs), compact disk –read writable (CD-RWs), DVDs, digital video recorders (DVRs), software, etc.

Department heads, or their designated approving agent, will authorize the adding of any networked component that is connected either directly to the County's Wide-Area-Network, indirectly connected via a Local-Area-Network segment, or attached to an existing computing system.

Using products that are not appropriately licensed for use by the County or those that violate the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software is prohibited.

13 Archive Data Protection

This section establishes for the protection and safeguarding of Riverside County data stored on backup media. In the field of information technology, backup refers to the copying of data so that these additional copies may be restored after a data loss event. Backups are useful primarily for two purposes: to restore a computer to an operational state following a disaster (called disaster recovery) and to restore small numbers of files after they have been accidentally deleted or corrupted.

The public rightly assumes and should be assured that the data in the possession of Riverside County government is secure and protected from unauthorized disclosure or use.

This covers all County data stored on backup media, including but not limited to:

13.1 Magnetic Tape

Magnetic tape has long been the most commonly used medium for bulk data storage, backup, archiving, and interchange. Tape has typically had an order of magnitude better capacity/price ratio when compared to hard disk, but recently the ratios for tape and hard disk have become a lot closer.

13.2 Hard Disk

The capacity/price ratio of hard disk has been rapidly improving for many years. This is making it more competitive with magnetic tape as a bulk storage medium. The main advantages of hard disk storage are the high capacity and low access times.

13.3 Optical Disk

A CD-R can be used as a backup device. One advantage of CDs is that they can hold 650 MIB of data on a 12 cm (4.75") reflective optical disc. (This is equivalent to 12,000 images or 200,000 pages of text.) They can also be restored on any machine with a CD-ROM drive. Another common format is DVD+R. Many optical disk formats are WORM type, which makes them useful for archival purposes since the data can't be changed.

13.4 Floppy Disk

During the 1980s and early 1990s, many personal/home computer users associated backup mostly with copying floppy disks. The low data capacity of a floppy disk makes it an unpopular choice since 2006.

13.5 Solid State Storage

Also known as flash memory, thumb drives, USB keys, compact flash, smart media, memory stick, secure digital cards, etc., these devices are relatively costly for their low capacity, but offer excellent portability and ease-of-use.

13.6 Remote Backup Service

As broadband internet access becomes more widespread, remote backup services are gaining in popularity. Backing up via the internet to a remote location can protect against some worse case scenarios, such as a county building burning down, destroying any backups along with everything else. A drawback to remote backup is the internet connection is usually substantially slower than the speed of local data storage devices, so this can be a problem for people with large amounts of data. It also has the risk of potentially losing control over sensitive data.

13.7 Backup Media Requirements

In order to ensure the recoverability of critical information, copies of Backup media shall be stored at a geographically separated County owned/leased facility, or with an authorized contracted data storage vendor. Departments or agencies may enter into agreements to store Backup data with another department and/or offer to provide reciprocal services. At no time will Backup media be stored at a personal residence or other personal property.

In the event that County Backup media is lost or stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, it must be reported immediately to the appropriate department or agency management and to the ISO.

14 Wireless Networking

Access to Riverside County networks via unsecured wireless communication mechanisms is prohibited. Only wireless systems that have been approved by the ISO, through the Wireless Design Review process, or have been granted an exclusive waiver, are permitted to be connected to Riverside County's networks.

This covers all wireless data communication devices (e.g., personal computers, cellular phones, PDA's, etc.) connected to any of Riverside County's internal networks. This includes any form of wireless communication device capable of transmitting packet

data. Wireless devices and/or networks without any connectivity to Riverside County networks do not fall under the purview of this policy.

14.1 Wireless Requirements

Wireless systems must meet the following requirements:

- Wireless deployment designs must be approved by the ISO and RCIT/Communications Engineering, via the Wireless Design Review process, or granted an exclusive waiver.
- All wireless equipment connected to Riverside County's networks (CORNET) or any departmental Local Area Network (LANs) must be coordinated with RCIT/Communications Engineering.
- Avoid advertising the presence of a Wireless Local Area Network (WLAN): The easier it is to find, the more likely it will be a target. Change the Service Set Identifier (SSID) so that it's not the factory default, and turn off SSID broadcasting. The RCIT Communications Bureau, at the direction of the ISO, will manage and assign all SSIDs. Access point (AP) antennas and power levels will be adjusted to avoid signal leakage to areas where coverage is neither required nor desirable.
- It is easy to spoof a device so that it looks like another device. Lost or stolen devices are also a severe threat. Media Access Control (MAC) address control alone is insufficient protection. Device-independent authentication, such as secured user names and passwords, which integrate with existing network directories or authentication schemes, will be implemented.
- Wireless data requires encryption. A minimum of 128 bit encryption is required. WEP (Wired Equivalent Privacy) is weak and does not meet this requirement. Advanced encryption protocols, such as WPA2, are necessary to meet the minimum security requirements.
- Use Access Control Lists (ACL) to limit WLAN Access to County resources.
- Do not place APs on desks or other locations where they can be easily accessed. Unscrupulous visitors or careless employees can easily move, replace, or reset the APs. Security cannot be assured in such insecure locations. Equipment will be placed in secure areas, such as a wiring closet.
- Actively monitor AP configurations. It's not sufficient to just configure an AP correctly; once configured, the AP must stay properly configured.
- The owning department will document periodic inspections of AP configurations.
- The ISO will perform periodic scans to detect and disable unauthorized APs. Active sniffing for these rogue devices is a critical operational requirement.
- Over a wireless LAN, an intruder can attack the wireless clients themselves in a peer-to-peer fashion. This attack can give the intruder network access by simply using a legitimate client as an accepted entry point. To address this issue, desktop firewalls

shall be deployed on all devices connected via wireless AP, along with network management tools that actively audit and manage the client before permitting access via the wireless LAN.

- Deploy real-time policy management. As they are deployed, wireless LANs will span entire campuses and incorporate multiple sites. Security policies (e.g., valid user lists or access rights) will naturally change. These changes must be reflected in real time throughout the wireless LAN to reduce the window of opportunity for intrusion and, more important, provide immediate lockdown of detected security holes.
- All WLANs will be routinely monitored. This is to verify that security configurations comply with this policy; to determine if devices are authorized; to identify unauthorized activity; and to maintain a current inventory of wireless devices.
- Network bridging must be disabled on all devices connected to a WLAN.

14.2 Definitions

- **AP:** Access point or base station of a wireless LAN.
- **MAC Address:** Media Access Control address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.
- **SSID:** Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the Basic Service Set (BSS). When one AP is connected to a wired network and a set of wireless stations, it is referred to as a BSS. The SSID differentiates one WLAN (wireless local-area network) from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network
- **User Authentication:** A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.
- **Wireless LAN (WLAN):** A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.
- **Spoof (Spoofing):** Electronically changing the packets sent from your computer so they appear to be coming from a different source. This is often used to hi-jack a connection or to impersonate another machine on a network.

15 Analog Lines

As part of the on-going security assurance efforts across the County, departments must closely track and monitor the installation and use of all analog telephone lines.

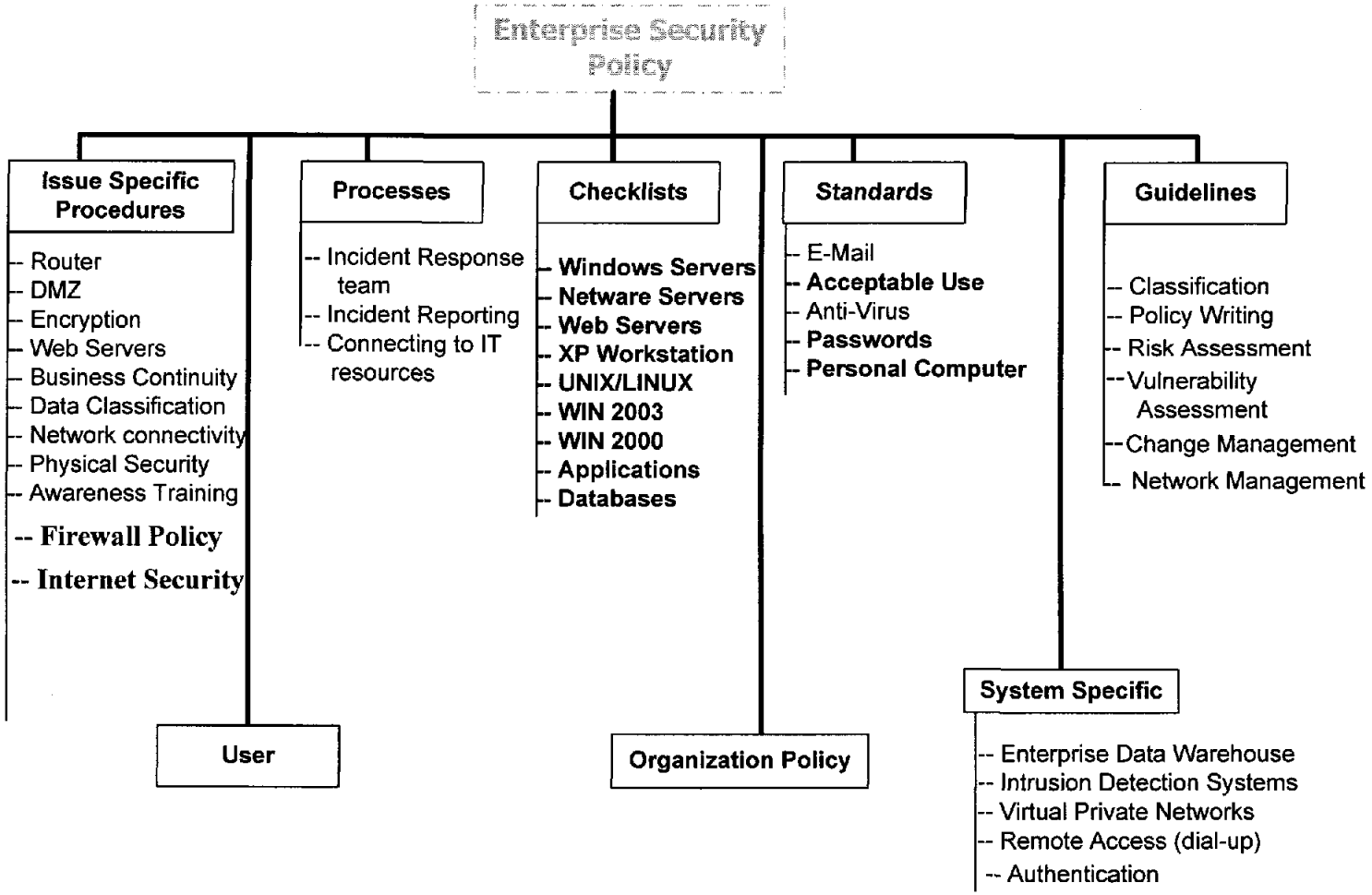
There are two important scenarios involving analog line misuse that we attempt to guard against through policy.

- The first is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it (also referred to as a "war dial"). If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside County premises, then there is the possibility of breaching the County's internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This potentially results in the exposure of sensitive information.
- The second scenario is the threat of anyone with physical access into a County facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted network of the County through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon County information to an unknown location. This could also potentially result in the substantial exposure of vital information.

Specific procedures for addressing the security risks inherent in each of these scenarios must be developed and fully documented by each department. Each department is responsible for establishing procedures and designating approval authorities who will be accountable for these lines. The senior IT person in each department is the default responsible agent. Department heads may designate anyone deemed appropriate within their department as an alternative Point of Contact for this function.

Appendix A

Department, Agency and District Required Procedures



Appendix B

Riverside County Enterprise Information Systems Security Policy

User Agreement

I have read, understand and am fully aware of the County of Riverside Enterprise Information Systems Security Policy; and I agree to comply with the terms of this policy. I also agree to remain informed of and comply with future revisions to this policy.

As a user of the County's information systems, you will have access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all users actively support and fully comply with the measures described in the Enterprise Information Systems Security Policy. Failure to comply can place the entire County network at serious risk; and users who fail to comply will be subject to disciplinary action.

Users of the County's information systems shall at all times act in accordance with all applicable laws and County policies, rules or procedures. Users shall not use County information systems in an improper or unauthorized manner.

User Name: _____

Signature: _____

Date: _____

Responsible Manager Approval Authority

Name and Title: _____

Signature: _____

Date: _____

This form shall be retained in department, district or agency files.

Appendix C

Riverside County Enterprise Information Systems Security Policy

Administrator Agreement

I have read, understand and am fully aware of the County of Riverside Enterprise Information Systems Security Policy; and I agree to comply with the terms of this policy. I also agree to remain informed of and comply with future revisions to this policy.

As an administrator of the County's information systems, you will have access to and responsibility for sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all administrators actively support and fully comply with the measures described in the Enterprise Information Systems Security Policy. Failure to comply can place the entire County network at serious risk; and administrators who fail to comply will be subject to disciplinary action.

Administrators of the County's information systems shall at all times act in accordance with all applicable laws and County policies, rules or procedures. Administrators shall not use County information systems in an improper or unauthorized manner.

Administrator Name: _____

Title: _____

Signature: _____

Date: _____

Responsible Manager Approval Authority

Name and Title: _____

Signature: _____

Date: _____

This form shall be retained in department, district or agency files.

Appendix D

Riverside County Enterprise
Information Systems Security Policy

Remote Access Agreement

I have read, understand and am fully aware of the terms of the County of Riverside Enterprise Information Systems Security Policy, especially as applied to remote users of the County's information systems; and I agree to comply with the terms of this policy. I also agree to remain informed of and comply with future revisions to this policy.

As a remote user of the County's information systems, you will have unique access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all remote users actively support and fully comply with the measures described in the Enterprise Information Systems Security Policy. Failure to comply can place the entire County network at serious risk; and remote users who fail to comply will be subject to disciplinary action.

Remote users of the County's information systems shall at all times act in accordance with all applicable laws and County policies, rules or procedures. Remote users shall not use County information systems in an improper or unauthorized manner.

Remote User Name: _____

Signature: _____

Date: _____

Responsible Manager Approval Authority

Name and Title: _____

Signature: _____

Date: _____

This form shall be retained in department, district or agency files.