County of Sacramento

Technology Review Group

Date: 12, April 2000

To: Information Technology Policy Board

From: Jim Person, Chair
Technology Review Group

Subject: Perimeter Security Policy

RECOMMENDATIONS:

That your Board:

1. Recognize the importance of perimeter security as an essential and critical wide area network component.

2. Approve the Perimeter Security Policy described in this document.

3. Establish a Perimeter Security Team responsible for the management of this environment.

BACKGROUND:

Securing Sacramento County's Wide Area Network (SCWAN) is essential. Malicious practices originating from outside of the County's sphere of control could potentially cause service interruption, data loss, data corruption, and/or security breach if security structures are not present or are ineffective due to dilution or compromise.

The function of this policy is to formally define Sacramento County's perimeter security and its architecture. This policy provides guidelines and procedures through policy by which this architecture and its supporting systems should be managed and maintained.

Although the County of Sacramento has an existing perimeter security architecture, this architecture has never been formally accepted. Current business needs require a written, accepted, and enforceable policy in order to accomplish business objectives without the dilution or compromise of perimeter security.

PERIMETER SECURITY POLICY:

This policy applies to those entities that are on the SCWAN. Existing agreements and legislative requirements will not be superceded by this policy. Business solutions should be investigated with the intent to meet the business needs without sacrificing security. Violations of this perimeter security policy will be reported to the Chief Security Officer for resolution.

The terms used in this document are defined in Attachment I. The strategies behind the following policy statements are detailed in Attachment II.

Policy:

1. Any external connection to the Sacramento County Wide Area Network shall come through the perimeter security's managed point of entry.

2. If determined safe by the Perimeter Security Team, outbound services will be initiated for internal addresses to external addresses.

3. Inbound services shall be negotiated on a case by case basis with the Perimeter Security Team.

4. Parties connecting to the SCWAN shall sign appropriate security agreements before connectivity is established.

5. The Perimeter Security Team is responsible for the perimeter security architecture, its resources, and its periodic auditing and testing.

Current exceptions:

Current exceptions are security risks and are not precedents for new service The following exceptions will be phased out within two years upon approval of this policy. Extension of the two-year phase out period can be evaluated by the ITPB on a case-by-case basis.

1. Existing modem connections to desktops within the WAN.

2. Existing departmental RAS (Remote Access Server) solutions provide direct access to departmental data or resources.

3. Existing AS5200 dialup directly accesses the WAN. (Current strategy is to move this connection to the DialNet, which would alleviate any security concerns).

4. Other external SCWAN connections identified by the Perimeter Security Team.

Requests for Services:

1. Written request for services should be sent to the Perimeter Security according Service Request Guidelines.

2. Requests for service will be completed within 5 business days or the department will be notified if the request is not completed by then.

Request Approval:

1. The Perimeter Security Team can implement requests that meet the requirements of this policy and other County policies and clearly do not place SCWAN resources at risk.

2. Requests, which would require interpretation of this policy or could potentially put SCWAN resources at risk, should be presented before the TRG for assessment and authorization.

Operating Guidelines:

Guidelines for the day to day operation of the perimeter security are detailed in Operating Procedures Manual maintained by the Security Perimeter Team.

PERIMETER SECURITY TEAM:

The Chief Information Officer will be responsible for appointing the members of the Perimeter Security Team. The team will be responsible for:

- Designing security solutions that secure the County's network, systems, and data.
- Providing an infrastructure which allows
  - public access to Internet systems;
  - vendor and business partner access to support purchased systems and provide electronic business capability with County Departments;
  - Inter-departmental access.
- Presenting security designs to the TRG for review.
- Identifying problems, alternative solutions, costs, and recommended course of action to the TRG.
- Managing all perimeter security systems.

POLICY UPDATES

Regular assessments will be conducted, by the Perimeter Security Team, of the perimeter security architecture and its policies to validate relevance and applicability to the current environment. Requests for perimeter security policy changes will come before the TRG for review and recommendation to the ITPB.

IMPACT OF IMPLEMENTING THESE RECOMMENDATIONS

Sacramento County began operating under a defacto perimeter security policy with the implementation of the firewall. The policies and procedures recommended in this document formalize this policy and recognize the authority to enforce perimeter security to protect County assets.

ATTACHMENT I
DEFINITION OF TERMS

Sacramento County Wide Area Network (SCWAN): the County network infrastructure and its resources as defined in Intranet below.

Internet: Public, cooperative, and self-sustaining facilities (public network) external to the County of SCWAN.

Intranet: Internetwork that is contained within an enterprise (private network). Any entity that has a connection to the SCWAN that is not going through the managed point of entry is considered part of the Intranet.

Extranet: Private network that securely shares information or operations with suppliers, vendors, partners, customers, or other businesses whose only connection to the SCWAN is through the managed point of entry.

Screened Subnet: A separated network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to internal resources that have County data, applications or services. A screened subnet is also known as a de-militarized zone (DMZ).

Managed Point of Entry: That point through which all network traffic external to the SCWAN passes (usually implemented using firewall technology).

ATTACHMENT II

PERIMETER SECURITY STRATEGIES

1. DENY ALL STRATEGY: WHAT IS NOT EXPRESSLY PERMITTED IS DENIED.

   Services as a general rule are denied unless they are expressly defined. The application of a "deny all" strategy suggests that only the required (and thereby configured) services will be available. All other unused services will be denied.

2. THE PRINCIPLE OF LEAST PRIVILEGE.

   The principle of least privilege is that an object (host, service, resource, subnet, etc.) should have the minimum privileges necessary to perform its assigned task and no more. A corollary of this principle is that systems should be configured so they require as little privilege as possible.

3. MINIMIZE PUBLICATION OF INFORMATION.

   Best business practice and strategy is to minimize the amount of internal network and resource information that is disclosed to the public Internet.

4. SINGLE ENTRY \ EXIT.

   Best business practice and strategy is to have a single point of entry to the Intranet. Multiple access points and therefore multiple access policies dilute the perimeter security and its capability to provide first line security.