CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

Network Security Management Standard

Information Security & Emerging Technologies

Last Revised: **06/13/2018**

Final

REVISION CONTROL

Document Title: CSUSB – Network Security Management Standard

Author: James Macdonell

File Reference:

Date	By	Action	Pages
06/12/08	J Macdonell	Created Procedures Guide	All
04/04/2018	ISET	Update and added scope to include cloud services	All
6/13/2018	J Torner & L Carrizales	Changes as recommended by ISET Subcommittee	All

Review/Approval History

Date	By	Action	Pages
	IT ISET Subcommittee	Approval	All
6/13/2018	ISET Subcommittee	Approve recommended changes	All
10/29/2018	IT Governance	Approved by Executive Committee	All

1.0 Network Security Management Standard

This standard establishes the process by which changes in the network security access controls are processed and includes, when appropriate, the authorization of a manager (MPP) when university information assets under the responsibility of the manager are exposed to the internet.

1.1 Scope

Access controls, network segregation, and the change control procedures described in this standard applies to all university information resources located on the campus premises as well as those provided by third party vendors (cloud providers). It includes physical as well as virtual networks and systems.

For the application of this standard, it is understood that even for completely virtualized environment, the security architecture should consist of multiple layers (logical or physical) of access control protection. These layers map to an internet exposed layer and internal layers that separate systems or resources that access and/or process data with different levels of security classification. Access and change controls at these layers should follow this standard.

1.2 Network Perimeter Security Standards

The network perimeter of CSUSB consists of three layers of protection: the Border Routers, the Edge Firewalls, and the Distributed Firewalls deployed across the internal network. Access Control Policies ("*firewall rules"*) at each layer manage access to University resources based on the appropriate level of protection and authorization. These Access Control Policies should be evaluated to follow the University Information Security Data Classification and Protection Standards.

1.2.1 Access Control Policies: Edge Firewalls and Distributed Firewalls

Access Control Polices ("firewall rules") must be implemented to allow only authorized access to resources

Network access for University resources is managed using of two firewall systems. The Edge Firewalls enforce Access Control Polices for University resources accessed from the Internet. The Distributed Firewalls enforce Access Control Policies for University intranet resources based upon the specific Virtual Local Area Networks (VLANs) in which they reside. The Edge Firewalls and Distributed Firewalls are intended to enhance the overall protection of all computer information systems. These systems are intended to supplement — not replace — proper configuration and maintenance for individual servers and computers. The continued use of host-based firewalls is expected and encouraged.

Access Control Policies implemented on the Edge Firewalls enforce access policies for resources accessed from the Internet. The Internet is considered a hostile network. Exposing University resources to the Internet significantly increases the risk of system compromise and unauthorized disclosure of information. Therefore, requests for changes to Access Control Policies that expose University resources to the Internet should be made with the approval of a manager. These

requests should also be carefully reviewed by the Information Security Office before being implemented on the Edge Firewalls.

Access Control Policies implemented on the Distributed Firewalls enforce access policies for campus intranet services. These policies should provide overall protection to all computer systems in a particular VLAN. They should be selected to ensure an acceptable level of protection to all computer systems in a particular VLAN without adversely affecting availability for authorized users and systems.

Existing Access Control Policies on both the Edge Firewalls and Distributed Firewalls should be periodically reviewed to ensure they follow the University Information Security Data Classification and Protection Standards.

1.2.2 Standard Segregation of Network Resources

In general, there are two categories of VLANs: Server VLANs and User VLANs. Server VLANs contain resources accessed from the Internet. User VLANs contain end-user systems.

Access Control Policies for Server VLANs should manage access to particular servers from both the intranet and the Internet. Server VLANs containing computers that store, process, or transmit critical, protected, or confidential information should be segregated from Server VLANs containing non-critical or public information.

Access Control Policies for User VLANs should prevent access from the Internet. That is, computers contained with User VLANs should not contain resources accessed from the Internet. However, some intranet exceptions may be allowed. User VLANs containing computers that store, process, or transmit critical, protected, or confidential information should be segregated from User VLANs containing non-critical or public information.

1.2.3 Request

It is important to select the Access Control Policies carefully and take in consideration the needs of all the users or assets in the VLAN. Changes to Access Control Policies can unintentionally permit unauthorized access to important or critical resources. Changes can also unintentionally deny authorized access. Additionally, Access Control Policies almost always require technical knowledge of networking and network protocols.

Changes to Assess Control Policies entail both business risks and technical pitfalls. Therefore, a designated technician — acting with the consent of an informed manager (or administrator) responsible for the computer resources contained in the affected VLAN — must submit all requests for changes to Access Control Policies.

All changes to Access Control Policies must be requested by submitting an electronic Network Work Order Request to the Telecommunications and Network Services network administrator.

Request must specify:

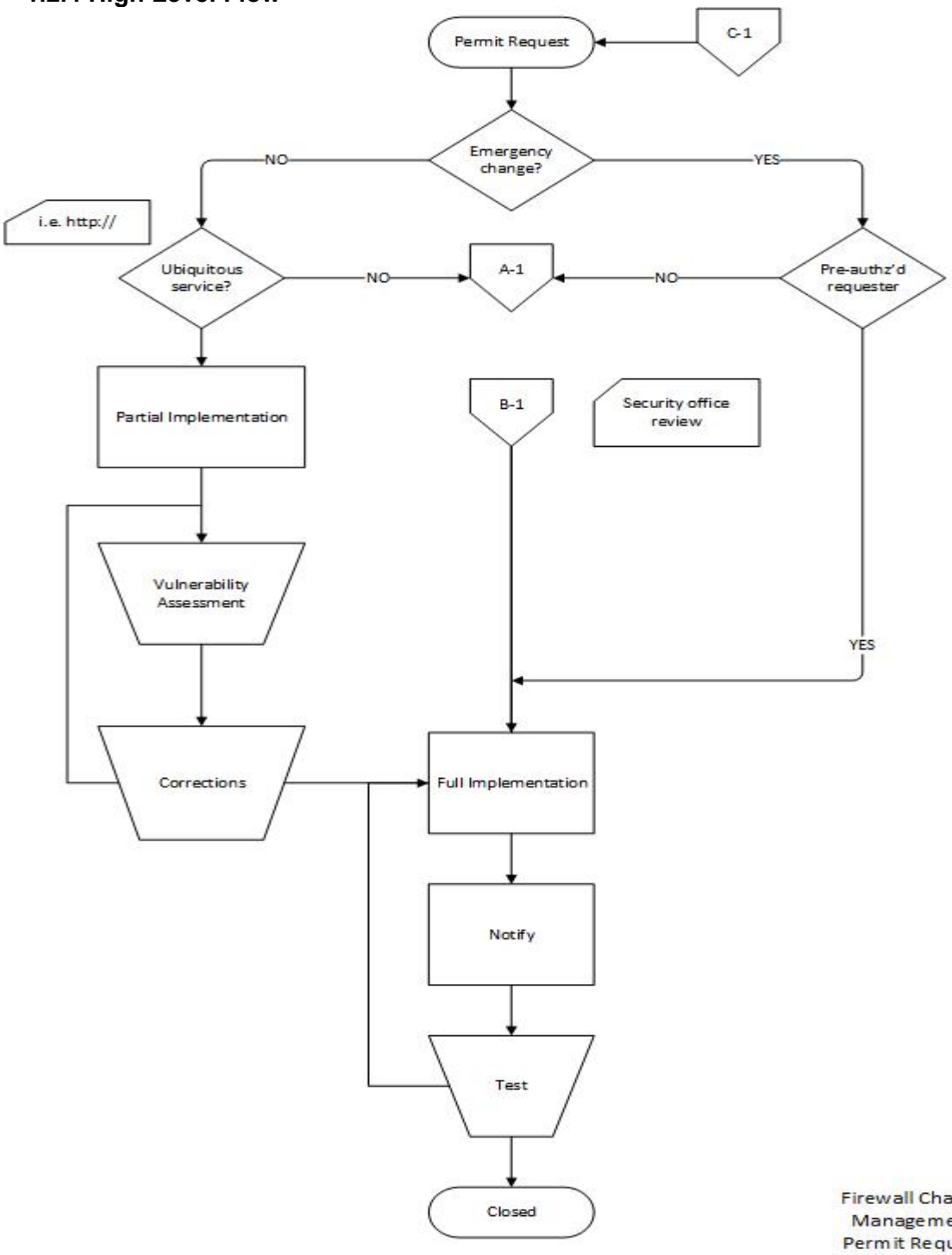
- the VLAN containing the asset being exposed (or protected),
- the name or address of the asset,

- the type of service to be exposed (or protected),
- the network address or range (not) authorized to access the service,
- and the intent of the request.

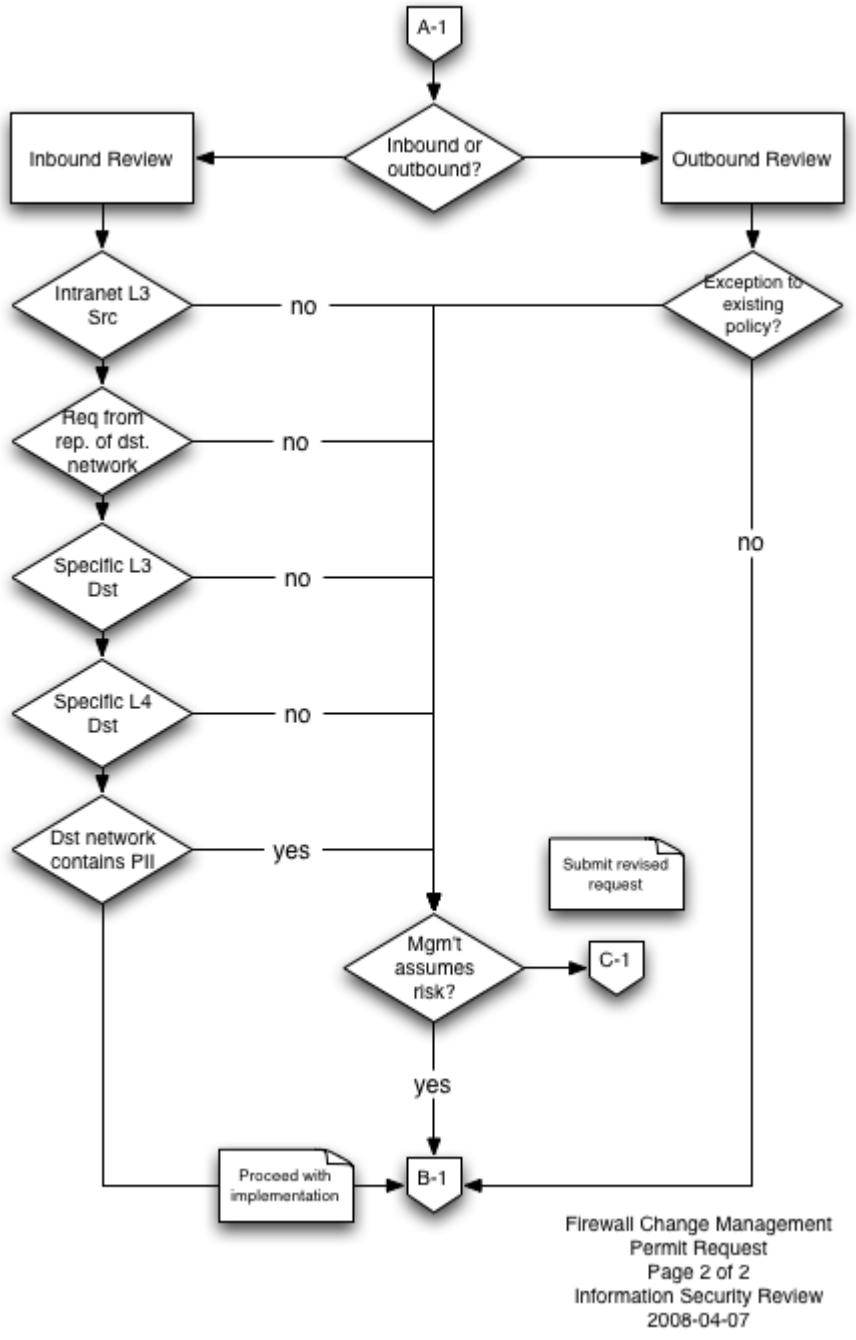
The Network Work Order Administrator will verify the authenticity of all Network Firewall Requests and submit the request to the Information Security Office. The Information Security Office will review the intended changes to Access Control Policies before they are implemented and provide recommendations as appropriate to the individuals responsible for the computer resources contained in the affected VLAN.

The manager (or administrator) of the computer resources assumes all responsibility for increasing the potential risk to assets by requesting and approving the implementation of specific Access Control Policies.

1.2.4 High Level Flow



1.2.5 ISO Review



See ISO Firewall Request Review as SVG

1.2.6 Implementation

In order to minimize the interruption of services to the campus, the Network Firewall Administrator will schedule all changes to Access Control Policy following the network maintenance schedule. The Network Firewall Administrator will inform the request initiator of the date when the changes to Access Control Policies will be implemented. The request initiator is responsible for testing the implementation and promptly notify the Network Firewall Administrator of any problems.

1.3 Access Control Policies: Border Routers

Routers are designed to pass traffic, not block traffic

The Access Control Lists (ACLs) or the Border Routers provides the first layer of protection for the network and computer information systems of the campus by enforcing appropriate Access Control Policies.

Prior to implementing any changes to Access Control Policies on the Border Routers, it is of critical importance to carefully assess the impact to the campus community — these changes affect the entire campus community. With this in mind, the following procedure has been adopted in an effort to minimize the potential negative impact originating from the implementation of changes to Access Control Policies on the Border Routers.

1.3.1 Change Process

Access Control Policies for the Border Router require careful consideration and must meet the following criteria:

- The restriction will have a minimum impact to the campus community
- The restriction must provide a significant reduction on a potential or identified security risk
- The restriction should be as specific as possible while also requiring no or minimal maintenance.

1.3.2 Guidelines

Given the nature of the device and its position in the network topology, the Access Control Policies implemented on the Border Routers should be:

- thought of in terms of "denied by default"
- robust so that they rarely change
- considerate of the stateless nature of ACL

Before implementing new Access Control Policies:

- Traffic related to the policy must be monitored in order to identify users or services that will be adversely affected. Alternative access or exception must be taken in consideration.

- Procedures for requesting an exception to the upcoming Access Control Policies must be developed

Immediately after new Access Control Policies are implemented:

- Network traffic affected by the new policies must be monitored in order to assess its efficiency.
- Impact to router performance must be evaluated.

1.3.3 Exceptions

Exceptions to the procedures to change Access Control Polices can be granted at the discretion of the Information Security Office only under extreme circumstances and when critical information systems may be at risk.

1.3.4 Traffic Monitoring

Information will be collected from the Border Routers, the Edge Firewalls, and Distributed Firewalls as permitted by Federal and State Law, and CSU and CSUSB policies for the purpose of detecting attacks, intrusions, malicious traffic, and any other network activity that may place the University and its information resources at risk.

Access to network flow information for a specific VLAN will be granted only with the authorization of the Information Security Office and the authorization of the manager (or administrator) responsible for the VLAN in question.

All network flow information will be maintained for a period no longer than 180 days from the time of collection.

1.3.5 Access Control Policy Audit

The Information Security Office will periodically audit Access Control Policies as during routine campus vulnerability assessments. The manager (or administrator) and the designated technician may be contacted in instances where there may be questions or concerns about a specific Access Control Policy.

1.3.6 Emergency Procedures

The Edge Firewalls and Distributed Firewalls run in a fail-over mode in order to provide firewall protection in the event of a hardware failure. However, in the event of a major disruption of network firewall protection, all identified managers and corresponding technicians will be promptly notified.

The Information Security Office may authorize the immediate implementation of new Access Control Policies when critical information systems may be at risk.