Solano Community College

Intrusion Detection and Prevention Department Policy

Purpose

The purpose of this policy is to define the use and management of intrusion detection and prevention for Solano Community College systems

Scope

This IT policy applies to devices exposed to the Internet

Definitions

Intrusion detection and prevention – a process performed by a device, software, or a combination, that actively monitors traffic, looking for suspicious activity, attempts at unauthorized access, and proactively blocks traffic deemed to be an attempted intrusion

Process

The internal Solano Community College network will run intrusion detection and prevention at the edge firewall level. It is a licensed feature on the firewalls, actively scanning for threats based on signatures and also by activity deemed threatening or suspicious. Attempts are logged at the firewall level and can be examined further, with the aid of the manufacturer's threat knowledge base to determine likelihood of compromise and possible remediations.

Revision History

Version:	Date:	Description:
1.0	10/7/2022	Initial document