

Idaho Technology Authority (ITA)

ENTERPRISE STANDARDS S2000 – SOFTWARE – DESKTOP, NOTEBOOK & MOBILE DEVICES

Category: S2130 – Anti-Virus/Endpoint Security (AV/EPS)

CONTENTS:

- I. [Definition](#)
- II. [Rationale](#)
- III. [Approved Standard\(s\)](#)
- IV. [Approved Product\(s\)](#)
- V. [Justification](#)
- VI. [Technical and Implementation Considerations](#)
- VII. [Emerging Trends and Architectural Directions](#)
- VIII. [Procedure Reference](#)
- IX. [Review Cycle](#)
- X. [Contact Information](#)
[Revision History](#)

I. DEFINITION

Anti-Virus (AV) desktop protection solutions have evolved to become Endpoint Security (EPS) solutions which encompass more of the overall security requirements for client computers and mobile devices. EPS is one facet of a defense-in-depth security strategy which is considered a best practice in protecting the overall enterprise network and its information as well as the specific information on the client computer itself. While AV was once a stand-alone application which protected a specific client from known malicious software, EPS includes a wider suite of defensive technologies supported by a management application where all the included features are administered.

II. RATIONALE

The State of Idaho holds vast amounts of information pertaining to its citizens and its actions in serving those citizens; therefore, the State has the responsibility to protect that information from loss, destruction or theft. Also, in keeping with the *National Strategy to Secure Cyberspace*, <http://www.whitehouse.gov/pcipb/>, the State of Idaho should secure the portions of cyberspace which we own, operate, and control. In doing so, we need to be able to identify threats as they occur, respond appropriately, and share the information within the State as well as with national-level security organizations which can then employ and enable all other appropriate organizations to respond accordingly. With a standard AV/EPS in the State of Idaho, any incidents of malicious software or activities detected by the AV/EPS will be centrally reported, responses can be quicker and shared across the agencies for

better protection of the State's information. Furthermore, economies of scale and efficiencies can be realized from the employment of one effective AV/EPS.

III. APPROVED STANDARD(S)

This Standard currently stands alone.

IV. APPROVED PRODUCT(S)

McAfee Total Protection for Endpoint, and its official updates

V. JUSTIFICATION

The Office of the CIO conducted detailed assessments of the top rated AV/EPS products and the McAfee products were rated higher than the other products. In fact, over the course of the past year, many agencies had made their own decisions to move to McAfee from other products. In addition, the majority of agencies already use McAfee products, greatly reducing the cost of transitioning to one standard. Finally, the centralized platform used by McAfee AV/EPS is highly regarded in the IT Security community, it offers comprehensive and flexible centralized management and reporting, plus it interacts with the enterprise-wide intrusion detection and vulnerability reporting products already in place at the State enterprise level.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

While the Total Protection for Endpoint is the standard, individual agencies may assess their own needs for the additional protections offered in related McAfee endpoint products (e.g., data or hard drive encryption, data loss remediation, etc.) but are not constrained from obtaining those additional protections from different manufacturers.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

Promising EPS technologies are rapidly expanding and changing and McAfee solutions are evolving quickly. Agencies should evaluate and employ those products which they determine will be beneficial to their security while not falling below the protection levels provided through Total Protection for Endpoint.

VIII. PROCEDURE REFERENCE

Guidelines for the use of Mobile Devices are outlined in [Information Technology Enterprise Guideline G540 – Mobile Devices](#).

IX. REVIEW CYCLE

Six (6) Months

X. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 332-1876.

REVISION HISTORY

07/01/13 – Changed “ITRMC” to “ITA”.

6/16/09 – Added Approved Standards and deleted Timeline.

Effective Date: June 25, 2008