# Idaho Technology Authority (ITA)

# ENTERPRISE STANDARDS – S3000 – NETWORK AND TELECOMMUNICATIONS

**Category: S3230 – SECURITY – SERVER SECURITY REQUIREMENTS**

---

**CONTENTS:**



## I. DEFINITION

Server security as used in this standard: a base configuration of server equipment that is owned and/or operated by any state agency. This standard covers public-facing web servers because of their exposure to internet attacks, but it also covers internal web servers as well as other application servers, file servers, and database servers.

Public-facing server: any server which hosts a website or application which is accessible from the internet.

## II. RATIONALE

Idaho State government is responsible for protecting sensitive and business-critical information on the government network. Each agency and the state government as a whole must ensure safe practices are in place to reduce the risk that information will be lost, stolen or changed. This standard provides direction on where to learn minimum configuration requirements for securing servers to reduce their risk to the many different attacks and misuses that target servers and the information they hold or process.

## III. APPROVED STANDARD

Internet-accessible servers will be configured to meet minimum security requirements as referenced in the series of Guidelines G950. This series will be under continuous development in order to cover basic security configurations of common server operating systems and function. The series will also be updated over time to better address changing security best practices and industry standards.

## IV. APPROVED PRODUCTS N/A.

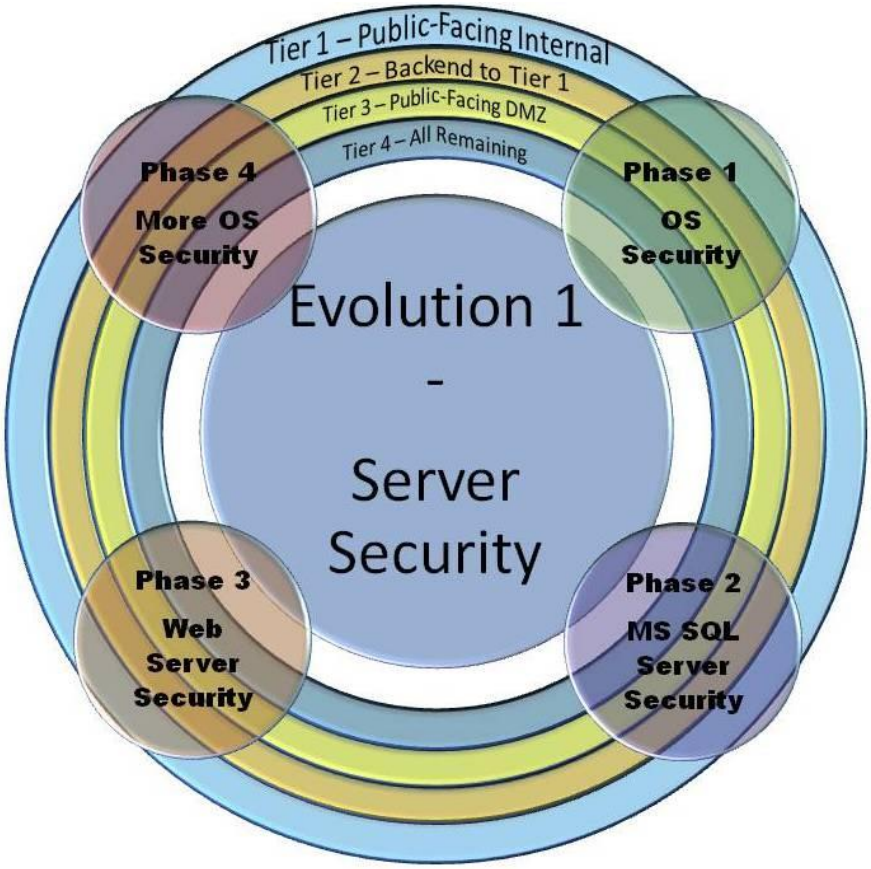
## V. JUSTIFICATION

The associated Guidelines, series G950, will provide minimum security configuration standards for server administrators to use while managing their servers. Using these guidelines will help provide better protection for sensitive state information as well as for citizen and employee personal data that the state holds. Some agencies may choose to use or are required to use stricter security standards; however, no agency may use less restrictive server configurations.

## VI. TECHNICAL AND SECURITY IMPLEMENTATION CONSIDERATION

A. The G950 Series Guidelines will be developed in phases. The initial planned phases include at least the following:

1. Initial Operating System (OS) hardening
2. MS SQL Server security
3. Web services security basics
4. More in-depth OS hardening




B. Agencies are encouraged to implement these security measures in Tiers. The Tiers reflect the servers which should be protected first based on their exposure to internet threats and their proximity to potentially sensitive information. The graphic below shows these phases and tiers. The Tiers include

1. Public Facing servers on the internal state network
2. Servers supporting those Internal Public Facing servers
3. Public Facing Servers on the Enterprise Demilitarized Zone
4. All other servers.

| Evolution | Short Evolution Description | Phase | Short Phase Description | Tier | Short Tier Description |
|---|---|---|---|---|---|
| Evolution 1 | Server Security | Phase 1 | Initial OS Hardening | Tier 1 | Public-Facing, Internal |
| | | Phase 2 | MS SQL servers (same Tiers as Phase 1) | Tier 2 | Backend to Tier 1 |
| | | Phase 3 | Web Servers (same Tiers as Phase 1) | Tier 3 | Public Facing, Ent. DMZ |
| | | Phase 4 | More OS (same Tiers as Phase 1) | Tier 4 | All remaining servers |
| Evolution 2 | Application Security | Phases | TBD | Tiers | TBD |
| Evolution 3 | Training Tracks for Sys Admins | Phases | TBD | Tiers | TBD |
| Evolution 4 | Move Public-Facing Servers to Ent DMZ* | Phases | TBD | Tiers | TBD |

C. In general, this standard covers the first evolution of four planned evolutions which are expected to take as much as five years to complete.

1. Server security,
2. Application security,
3. IT training track options which will enhance security skills,
4. Move all public-facing servers to the enterprise DMZ (unless a better option is developed)

## VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

In order to maintain secure server configurations, administrators should open only those ports and enable only those services which are specifically required for applications on any given server. Some Operating Systems are defaulted open; unnecessary ports and service must be disabled; however, other OS's, to include newer Microsoft Operating Systems, are defaulted to a secure mode and the required ports and services must be enabled.

## VIII. PROCEDURE REFERENCE

Guideline G950 Series.

## IX. REVIEW CYCLE

Six (6) Months

## X. CONTACT INFORMATION

OCIO Security Team, 332-1505.

## REVISION HISTORY

07/01/13 – Changed "ITRMC" to "ITA".

Approved by ITRMC June 23, 2010