

DTS Bulletin

Owner: Security Management Division

Number: 3120

Issue Date: 05/29/2008

Revised: 12/22/2008

HOSTED PROJECT SECURITY REQUIREMENTS AND RECOMMENDATIONS

Section 1 – Introduction

The Department of Technology Services (DTS), Security Management Division (SMD), developed high level security requirements and recommendations for systems hosted at DTS. This Bulletin applies to hosted environments that process, transmit, and/or store confidential, sensitive, or personally identifiable data.

Section 2 – Standard Requirements

A. Hosted Project Security Requirements

Listed below are the security requirements for any project containing public facing applications:

1. Network Architectures: SMD approves the below two network architectures. Please refer to [DTS Bulletin 3117 – Network Architecture Standard](#) for detailed information.

Firewall with Public-Facing Web Service Ports Open	Public Facing DMZ Tier 1	Firewall with Application Ports Open	Application Tier 2	Firewall with Database Ports Open	Data Tier 3
--	---------------------------------	--------------------------------------	---------------------------	-----------------------------------	--------------------

Firewall with Public-Facing Web Service Ports Open	Public Facing DMZ (Proxy) Tier 1	Firewall Application Ports Open	DMZ & Application & Data Tier ONLY for z/OS Tier 2
--	---	---------------------------------	---

2. Isolated virtual local area networks (VLANs) must exist per customer; it is desirable that each customer project be implemented in its own VLAN. Due to performance concerns of DTS firewalls, however, isolated VLANs per customer are appropriate.
3. Data repositories containing confidential, sensitive, or personally identifiable information must reside on a firewalled VLAN separate from the DeMilitarized Zone (DMZ) & application tier(s).
4. Provide detailed network architecture diagrams and data flow diagrams, including ports, protocols, and hardware placement, prior to procurement or implementation of any

device. This documentation should be provided to your DTS customer account representative and/or project manager, the earlier the better, so that security concerns can be brought to light mitigating any delay to the project schedule. The account manager and/or project manager will provide the documents to the appropriate DTS project resources.

5. No database management systems are allowed on a public Internet accessible network.
6. Web services may not be installed on database or data repository servers. Web services may be installed on application servers if communication traverses either a proxy server or web server in the public facing DMZ first.
7. Authentication devices cannot reside in the DMZ; e.g., Domain Controllers and Active Directories.
8. Systems that require outbound email notifications must utilize the DTS Simple Mail Transport Protocol (SMTP) relay service.
9. Systems must adhere to DTS security and system configuration requirements, which includes but is not limited to DTS Bulletin 3126 – Server Security Standard and 3128 – Virtual Server Security Standard. Please notify your DTS Customer Representative for access to these documents.
10. Systems that process, store, and/or transmit payment card data must adhere to current Payment Card Industry (PCI) standards. The customer or vendor responsible for building and/or designing the system must provide DTS with documentation of the system's PCI compliance prior to implementation.
11. Firewall ports are closed by default for testing, development or production environments. Requests for "all firewall ports to be opened" will be denied. Request specific ports or a range of ports as early as possible.
12. Firewall port and access control list request changes should be made via a service request with the [Firewall and Access List Request Form \(DTS 363\)](#) attached. Please refer to [DTS Bulletin 3121 – Firewall and Access List Request Procedure](#) for detailed information.
13. Approval by the information security officer (ISO) of the **data owner** is required, prior to implementation on all service and change requests involving:
 - a) Consulting for security or operational recovery
 - b) Confidential or sensitive data
 - c) Dial-in lines
 - d) Non-state users accessing the system/data
 - e) Firewall port or access list requests
14. System data must be classified by the customer per the [State Administrative Manual \(SAM\) section 5320.5](#) and disclosed to your DTS customer representative or project manager. Customer Managed Services, also known as SB 954, and hosted systems

containing unclassified data will adopt the most restrictive security measures by default. These security measures may result in additional costs to the customer. Refer to [DTS Bulletin 3113 – Data Classification Standard](#) for further details.

15. Confidential, sensitive, and personally identifiable information must be encrypted in transit and at rest while in publicly accessible DMZs. Encryption must adhere to the [Federal Information Processing Standard Publications \(FIPS\) 140-2](#).
16. No direct public access to the application and database tiers is permitted.
17. Publicly accessible front-end servers (web or web/application) may never have mapped network drives to back-end database servers.
18. Customer Virtual Private Network (VPN) accounts to the hosted environment may not be shared. If the VPN account is requested for the customer's *vendor* to access the hosted environment, the customer ISO must approve the service request. Hosted environments must subscribe to the DTS VPN service; a third party VPN connection may not be established.

B. Hosted Project Security Recommendations

Listed below are recommendations for hosted projects:

1. Confidential, sensitive, and personally identifiable information should be encrypted while traversing the public Internet. Encryption should adhere to the [Federal Information Processing Standard Publications \(FIPS\) 140-2](#).
2. Provide notice to DTS **prior** to application patching and/or maintenance so that technicians are aware and do not take unnecessary actions. This applies to all system environments; e.g., test, development, training, pre-production, or production.

C. DTS Security “Facts”

Listed below are routine DTS security activities affecting hosted projects:

1. Intrusion Prevention Systems (IPS) is active at the DTS perimeter. IPSs are not host-based.
2. Vulnerability scans of production servers take place regularly. Reports can be shared with customers upon request. A one-hour consulting rate fee will be charged for this service.

D. Glossary

Listed below is SMD's interpretation of some Information Technology terms and/or concepts:

Common Term/Concept	SMD Term/Concept
Internet facing web tier	Demilitarized Zone (DMZ)
World Wide Web	Public Facing
<i>n</i> -tiered architecture tiers or layers	Tiers
Inter Agency Internet or Intranet	CSGNet

Section 3 – Applicability and Exclusions

- A. Intranet web service applications, via CSGNet, are not held to the above architectural requirements.

This Bulletin does not apply to systems in the COEMS environment.

- B. Exceptions to this Bulletin must be documented and will be considered on a case-by-case basis. Requests for an exception to this Bulletin must be submitted via the DTS Policy/Standard Exception Request Form, DTS 358. Please refer to DTS Bulletin 3503 – Information Security Exception Request Procedure for detailed information. Direct any questions regarding the applicability of this Bulletin to the SMD. Please notify your DTS Customer Representative for this form and request procedure.

Section 4 – Auditing and Reporting

- A. Auditing may be performed on a periodic or random basis by the SMD or its designees. In the event an audit determines this Bulletin is not being applied, notification will be sent to the appropriate person for remediation.
- B. Any known violations of this Bulletin must be reported to the DTS Chief Information Security Officer and the reporting employee's immediate supervisor.

Section 5 – Authority/Reference

DTS Policy 3100 – Asset Protection Policy

[3113 – Data Classification Standard](#)

[3117 – Network Architecture Standard](#)

[3121 – Firewall and Access List Request Procedure](#)

3126 – Server Security Standard (Please notify your DTS Customer Representative for this document.)

3128 – Virtual Server Security Standard (Please notify your DTS Customer Representative for this document.)

DTS Bulletin 3503 – Information Security Exception Request Procedure (Please notify your DTS Customer Representative for this document.)

Policy/Standard Exception Request Form, DTS 358 (Please notify your DTS Customer Representative for this form.)

[Firewall and Access List Request Form \(DTS 363\)](#)

[Federal Information Processing Standard Publications \(FIPS\) 140-2](#)

[State Administrative Manual \(SAM\) section 5320.5.](#)