

VIRGINIA DEPARTMENT OF MOTOR VEHICLES

SECURITY ARCHITECTURE POLICY

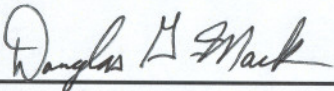
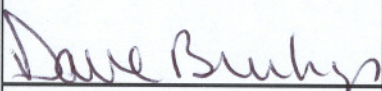

03/27/09 Version

Approved April 30, 2009



+ REDACTED VERSION +

**Approval of Enterprise Security Architecture Policy
(03/27/2009 Version)**

		
Douglas G. Mack IT Security Director ISO	Dave Burhop Assistant Commissioner CIO	D.B. Smit Commissioner Agency Head
4/21/09	4-24-09	4-30-09
Date	Date	Date

SECURITY is not complete without U!



Enterprise Security Architecture Policy

03/27/09 Version – Approved 04/30/09

1) Purpose

***** =
Redacted

The *DMV Enterprise Security Architecture Policy* is designed through concepts of enhanced security and standardization to be a core set of principles required to provide maximum uptime to applications and customers interacting with the DMV infrastructure.

To that end, DMV's *Enterprise Security Architecture Policy* is a service-based architecture utilizing a variety of techniques to provide this service level. DMV provides high-availability services to the mainframe, databases, and a variety of other DMV systems through this infrastructure.

2) Authority

DMV's *IT Security Policy* is the source for this *Enterprise Security Architecture Policy* and also provides the context for it.

Additional sources of authority are:

Code of Virginia § 2.2-603(G) (Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032. (Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

Code of Virginia, §2.2-2009 (Additional Powers of the CIO relating to security)

Code of Virginia, §2.2-2457 (Information Technology Investment Board)

Code of Virginia, §2.2-2827 (Restrictions on State employee access to information Infrastructure)

Code of Virginia, §2.2-3803 (Administration of systems including personnel information; Internet privacy policy)

Code of Virginia, §18.2-186.6 (Breach of personal information notification)

IT Information Security Policy (SEC500-02) (07/17/2008)

IT Information Security Standard (SEC501-01) (07/31/2008)

IT Security Audit Standard (SEC502-00) (01/11/2007) (Compliance Date: 02/01/2007)

IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511-00) (07/01/2007)

Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (SEC514-03) (03/15/2008)

Internet Privacy Guidelines (SEC2001-02.1) (02/27/2001)

IT Contingency Planning Guideline (SEC508-00) (4/18/07)

IT Data Protection Guideline (SEC507-00) (7/02/07)

IT Logical Access Control Guideline (SEC509-00) (4/18/07)

IT Personnel Security Guideline (SEC513-00) (2/15/2008)

IT Risk Management Guideline (SEC506-01) (12/11/2006)

IT Risk Assessment Instructions- Appendix D (SEC506-01) (12/14/2006)

IT Security Audit Guideline (SEC512-00) (12/20/2007)

IT Security Threat Management Guideline (SEC510-00) (07/01/2007)

IT Systems Security Guideline (SEC515-00) (07/17/2008)

Enterprise Architecture Policy (EA 200-00) (07/20/2006)

Appendix B: ETA Change- Exception Request Form

Enterprise Technical Architecture Standard (ETA 225-02) (04/01/09)

Statewide Implementation of Electronic Commerce (COV ITRM Policy 95-1) (08/08/1995)

3) Scope

All person or entities authorized to transact business, access, use, provide, or receive information contained in any DMV information system, record set, or electronic communication system are subject to this policy.

This includes, but is not limited to:

- a) Employees (full-time, part-time, wage employees),
- b) Contracted personnel (contractors, consultants, vendors, or temps),
- c) Non-employees (volunteers or interns).

4) Enforcement

Classified employees may be subject to disciplinary action up to and including discharge, under the Commonwealth's Standards of Conduct; and wage employees, contractors and consultants assigned to or working for the agency may be subject to administrative and contractual sanctions. Criminal or civil action may be initiated in appropriate instances.

5) Violation of Law

All known violations of the law shall be immediately reported to DMV Special Investigations Unit (SIU).

6) Background

DMV's Security Architecture Policy is based on the multi-tier application deployment model and a multi-level security model. These models provide a disconnect between user activity and the secured information that DMV maintains. The DMV's *Security Architecture Policy* provides methods to programmatically access information stored in DMV databases, host (mainframe) systems, and file stores. These methods provide risk mitigation and confidence that data is protected and accurate when accessed and delivered. It also provides a means to audit what data was accessed and by whom.

DMV's *Security Architecture Policy*, from a security perspective, is based on the security principles of "Least Privilege". The security model employed is based on best practices published by the NSA, NIST, Center for Internet Security and accredited security organizations such as ISC2 and SANS. These defined security models are applied to workstations, servers, applications and other elements of the infrastructure.

DMV is very restrictive with security policies. DMV only provides detailed security information on an as-needed basis. DMV will decide which security information is to be shared or released based on Commonwealth of Virginia security and architecture policy and *DMV IT Security Policy*.

DMV follows the guidelines provided in the Commonwealth of Virginia (COVA) Information Technology ITRM Security policies, standards and guidelines. The reference URL for these ITRM directives are found at:
<http://www.vita.virginia.gov/library/default.aspx?id=537> under the Information

Security heading.

Additionally, Commonwealth ITRM Enterprise Architecture guidance is found at: <http://www.vita.virginia.gov/oversight/default.aspx?id=365>.

Additionally, please review both of these sources of security architecture governance by reference to the templates and documentation for non-ITRM security found at <http://www.vita.virginia.gov/library/default.aspx?id=5520#security> .

With the passage of time, the exact URL may be changed, however the DMV governance process will published corrections to these URLs as they may be superseded, however vendors and other parties are to refer the ITRM and non-ITRM sections of the VITA Partnership Library <http://www.vita.virginia.gov/library/> for current information as it is needed.

In addition to Commonwealth of Virginia sources of security architecture, the requirements for development and implementations of security and architecture controls have been developed by reference to NIST Special Publication 800-53, revision 1. Over time different elements of these controls may be redacted or incorporated without notice.

All security and architecture guidelines published by the Commonwealth of Virginia and the Virginia Department of Motor Vehicles must be followed with current and proposed solutions. These requirements are set forth in the following subheadings below.

7) General Security Architecture Policy Requirements:

- a) DMV does not allow direct connections from outside sources to internal systems.
- b) DMV requires multi-level security models for risk minimization. For reference see: http://en.wikipedia.org/wiki/Multilevel_security. This requires segregation of differing risk levels using accepted techniques for security compartmentalization. Please refer to the following links for reference:
 - i) <http://www.cs.stthomas.edu/faculty/resmith/r/mls/index.html>
 - ii) <http://nsi.org/Library/Compsec/sec0.html>
- c) All externally and most internally available applications are designed in a multi-tier security model. The tiers are hosted on separate hardware resources and are separated by independent firewalls. These are not application layers but independent operational tiers that only can communicate with one another in distinct and prescribed ways. For reference information on the multi-tier security model please refer to:

- i) http://en.wikipedia.org/wiki/Multitier_architecture,
- ii) <http://www.microsoft.com/belux/msdn/nl/community/columns/hyatt/ntier1.mspx>
- d) No http proxy based applications are allowed.
- e) DMV restricts the IP application ports that are allowed to traverse networks and segments. It should not be assumed by an application has access to any port unless this security architecture policy specifically describes such interaction.
- f) DMV does not allow dynamic port allocation applications.
- g) DMV considers any machine that is directly accessed by an outside entity as a perimeter device and restricts accordingly.
- h) DMV does not allow the sharing of security credentials for user access to DMV systems. This includes both DMV internal users and external users.
- i) DMV restricts network services that traverse LAN and WAN networking segments.
- j) Direct remote access to any computer is not allowed.
- k) Standalone modems are not allowed
- l) Vendor provided remote control applications are not allowed.
- m) Servers and User PC's are restricted from residing on the same network segment.
- n) Any proposed system or optional configuration must have an automatic restart process for connection failures or if the back end systems are unavailable.
- o) System must provide future growth estimates and hardware requirements to support future growth and scalability.
- p) Any proposed system or optional configuration that requires a CSC Local Server must utilize a Virtual Server *****. No physical server will be allowed to be deployed locally to CSCs. Desktop systems are not utilized to provide server type services.
- q) *****
- r) Any customer record information that is access must be encrypted via known industry security methodologies and be fully documented.

s) *****

- t) Any proposed system or optional configuration must conform to the DMV Base Network Configuration that will be defined as VITA Partnership transforms our current network infrastructure.

8) Application Authentication Security Architecture Policy

Application authentication is handled differently based on where the application provides services and the characteristics of the service provided. Application Authentication & Authorization is provided by the following means based on specific use:

- a) DMV requires one of the authentication methods be selected by all current or proposed applications. No standalone user database are allowed without one of these authentication methods:
 - i) Microsoft Active Directory: Internal Application Authentication. This is not A/D synchronization resulting in an application user store and an A/D user store, but is consumption of the application of the existing A/D groups. Microsoft Active Directory usage is a Commonwealth authentication standard.
 - ii) DMV Employee PIN: Internal Application Authentication. Typically HTTP based applications.
 - iii) RSA SecurID FOB access: External Applications provided via DMV's web site, extranet system applications, and remote access for DMV Employees and trusted contractors.
 - iv) Future – the implementation of consumer based multi-factor based on security risk is being considered for implementation.

9) Remote Access Authentication Security Architecture Policy

- a) Remote access to the current or proposed system will be provided by devices and means identified by the IT Security Director (Information Security Officer - ISO).

b) *****

- c) For vendor requested connections to DMV, DMV will provide the remote access software that will be used. This software will allow the Vendor to remotely administer the servers related to their product.

d) *****

- e) Remote Data transfer connections must be secured via VPN or a method approved of by a security classification and sensitivity assessment by the DMV IT Security Director (Information Security Officer - ISO). These connections are regarded as severely restricted which will be treated as perimeter connections and firewalled with security applied accordingly.

10) Platform Infrastructure Security Architecture Policy

Platform Infrastructure Description

Previously the Security Architecture Policy, described how a multi-tiered security model is used. This security Policy also includes multi-level security aspects that protect data on one level from data on another level.

DMV utilizes Windows based servers as Presentation, Business Logic, and Data Access servers. DMV Servers are secured based on current industry standards provided by the NSA, SANS Institute, etc, as well as those published by VITA. Servers are designed with standardization across all machines. *****

The following are requirements for the platform infrastructure (multi-tiered and multi-level security) implemented at DMV for all systems:

- a) General tier requirement: NO direct access to any Data Access Tier information or services is allowed from either the Client or Presentation tiers.
- b) General tier requirement: All tiers are separated by firewall access control list rules
- c) General tier requirement: The presentation of an application to a client (whether as a separate application, as a browser-based presentation, or as another type of client device) is not to be counted as a presentation tier. The concept of a presentation tier is a hosted instance and is not a browser/client presentation of a user interface. The presentation tier is some instances would be the web server hosting the user interface to a web browser. It would not be the web browser itself. Additionally, terminal services as a client is not a tier, but a terminal services server hosting terminal services to connected clients would be a tier.

- d) General tier requirement: Applications must be architected in an n-tier configuration with at least 3 tiers (presentation, business logic, and data access).
 - i) A tier is not solely a software layer.
 - ii) A tier (see references above in 6) Background) is required to run on separate hardware resources and connections between such tiers are proxied through firewall and other security access.
 - iii) It is not allowed to have 2 software layers compiled and running on one tier (i.e. Presentation and Business logic layers running on Business Logic tier, or Business Logic and Data Layers running on Business Logic tier etc.).
 - iv) A tier is determined by operational separation (hosting) not by how a software layers is used (i.e. Hosting of the product or application requires a minimum of 3 tiers; it is not an optional component).
- e) Direct connections through tiers (i.e. client directly to data) are not permitted.
 - i) Access to the different tiers must be capable of being fully proxied. No tunneling or proprietary transport mechanisms are to be utilized.
 - ii) Each tier MUST have a documented and full featured API utilizing industry standard interfaces that are fully compatible with DMV's application infrastructure. This API must be licensed and available for DMV consumption.
 - iii) Communications between tiers should be TCP/IP port based connections.
 - iv) Application integration must occur via an API based Programmatic Methodology. "Screen Scraping" and HLLAPI techniques are not permitted.
- f) General tier requirement: Data transfer connections are subject to data access limitations described in the Application Tier structure presented in the Security Architecture Policy System Description and must be designed according to these requirements.
- g) DMV Architecture Security Policy tier structure:
 - i) Client Tier: Application front-end run by the user. Typically a web browser or smart client. This layer does not count as a tier/separation in determining if a tier is 3-tier or n-tier compatible.
 - ii) Presentation Tier: Content displayed to the user. IIS web server. This includes all UI access presented for client input and evaluation. Presentation tier to Business Logic Tier is physical hardware resource separation through a

firewall. It is not permitted that a presentation application layer exists on a services or data tier.

- iii) Business Logic Tier: Middleware layer that provides connectivity to backend systems for the Presentation Tier. This includes all business logic that is evaluated for decisions to process data. Business Logic Tier to Data Tier is physical hardware resource separation through a firewall. It is not permitted that business logic be presented on the presentation tier. It is not permitted that business logic exist as data in the data tier. It is not permitted that data be stored on the Business Logic tier.
- iv) Data Access Tier: Layer that provides data storage for DMV information. Databases, Host Systems, Files Storage, etc. This includes all data that is owned by the data owner of record for a DMV sensitive or non-sensitive system. Business Logic Tier to Data Tier is physical hardware resource separation through a firewall. It is not permitted that data be stored or maintained on a business logic or the presentation tier. It is not permitted that business logic exist as data in the data tier. It is not permitted that data be stored on the Business Logic tier.

11) Application Development Security Architecture Policy

- a) DMV does not deploy any Java revisions on the Enterprise Application Infrastructure servers.
- b) DMV does not deploy any Middleware clients (i.e. ODBC, Oracle, or SQL Server Client) to the servers unless it is a Business Logic tier server.
- c) DMV provides custom components to access the Data Access stores in place of the standard DACs provided by Microsoft.
- d) DMV prefers data access to be performed via web services through the Business Logic tier, but offers other custom components as an alternative for high-volume data access through the Business Logic tier.
- e) Application access to these COV legacy systems for access to COV customer records of account is provided by an API based programmatic approach or web services that are supplied by the Business Logic tier. Customer records of account are controlled by business decisions made by the system and data owners of record.
- f) Applications must not utilize any proprietary storage format and/or encryption routines that are not readily available for use by DMV's development staff to integrate applications with existing and/or new systems.

- g) Screen scraping or macro based solutions are not allowed. All communication to other systems must take place via a programmatic approach.
- h) Any proposed system or optional configuration and associated peripherals must be compliant with and utilize the Onbase system for, at a minimum, document acquisition, storage, workflow, and retrieval. DMV is licensed to utilize the Onbase application API for building custom interfaces to Onbase.

12) Personnel Roles required by the above Security Architecture requirements

DMV separates many administrative roles to ensure that proper staff requirements and expertise are utilized effectively.

Application Administrator/Supervisor

The designated user to administer the application side of the solution. This user would not have direct console access to the system servers. This user would typically be an area supervisor or manager.

Server Administrator

Typically responsible for the Hardware and Operating systems on Network Services Servers.

Would be responsible for:

- i) Server hardware and operating system configuration and maintenance
- ii) Server system disaster recovery
- iii) Network account management
- iv) Network access
- v) Server health monitoring

Database Administrator

Would be responsible for:

- i) Database table configuration
- ii) Database table access
- iii) Database administration

iv) Database disaster recovery

Software Development

Would be responsible for application design and maintenance. Would not be expected to manage applications.