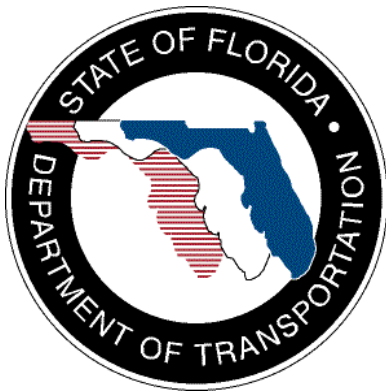


**SunGuide<sup>®</sup>:**

## **Software Security Plan**

**SunGuideSMD-SSP-1.0.0 (Working Final)**



Prepared for:

Florida Department of Transportation  
Traffic Engineering and Operations Office  
605 Suwannee Street, M.S. 90  
Tallahassee, Florida 32399-0450  
(850) 410-5600

August 19, 2010

<b>Document Control Panel</b>			
File Name:	SunGuideSMD-SSP-1 0 0(WorkingFinal).docx		
File Location:	SunGuide CM Repository		
	<b>Name</b>	<b>Initial</b>	<b>Date</b>
Created By:	Tucker Brown	TJB	07/27/2010
Reviewed By:	Ken Irvin	KDI	07/29/2010
	Robert Heller	RWH	07/29/2010
	Robert Heller	RWH	08/18/2010
	Tucker Brown	TJB	08/18/2010
	Ken Irvin	KDI	8/18/2010
Modified By:	Tucker Brown	TJB	08/16/2010
Completed By:			

## Table of Contents

<b>List of Figures .....</b>	<b>ii</b>
<b>1. Scope.....</b>	<b>1</b>
1.1 Document Identification.....	1
1.2 Project Overview .....	1
1.3 Related Documents .....	2
1.4 Contacts.....	2
<b>2. SunGuide Source Code Protection .....</b>	<b>3</b>
2.1 SwRI Source Code Storage.....	3
2.1.1 Source Code Repository.....	3
2.1.2 Desktop Security .....	3
2.1.3 Laptop Security .....	3
2.1.4 Copies of Delivery Media.....	4
2.2 Physical Security .....	4
2.2.1 Campus Security .....	4
2.2.2 Building Security .....	4
2.2.3 Lab Security.....	5
2.2.4 Server Security.....	5
2.3 Network Security .....	5
2.3.1 Network Topology .....	5
2.3.2 Network Access Rules.....	6
2.3.2.1 Public Network to Private Network.....	6
2.3.2.2 Private Network to Public Network.....	6
2.3.2.3 DMZ to/from Other Networks .....	6
2.3.3 Physical Access .....	6
2.3.3.1 Physical Access to the Private Network.....	7
2.3.3.2 Physical Access to the Division DMZ.....	8
2.3.3.3 Physical Access to the SwRI Visitor Network .....	9
2.3.3.4 Virtual Private Network (VPN) Access to Private Network .....	9
2.3.3.5 Outbound VPN Access from the Private Network.....	9
2.3.4 Policy Enforcement.....	9
2.3.5 Firewall Maintenance .....	9
2.3.6 Password Policy .....	9
2.3.7 Server Backup Policy.....	10

Attachment A – Division 10 Account Request Form  
Attachment B – Division 10 DMZ Authorization Form  
Attachment C – Division 10 Network Security Policy Waiver Form

## List of Figures

	<b>Page</b>
Figure 1-1 – High-Level Architectural Concept.....	1
Figure 2-1 – Logical View of the SwRI Division 10 Network.....	5

## **List of Acronyms**

AM	.....Ante Meridien
ADS	.....Automation and Data Systems
ATMS	.....Advanced Traffic Management Systems
CD	.....Compact Disk
CFE	.....Client Furnished Equipment
CT	.....Central Time
CM	.....Configuration Management
DVD	.....Digital Versatile Disk
DMZ	.....De-Militarized Zone
FDOT	.....Florida Department of Transportation
GFE	.....Government Furnished Equipment
ITC	.....Information Technology Center
ITS	.....Intelligent Transportation Systems
ITN	.....Invitation to Negotiate
PM	.....Post Meridian
PM	.....Project manager
QA	.....Quality Assurance
SPM	.....Software Project Manager
SSP	.....Software Security Plan
SWA	.....Standard Written Agreement
SwRI	.....Southwest Research Institute
TxDOT	.....Texas Department of Transportation
VPN	.....Virtual Private Network

### Revision History

<b>Revision</b>	<b>Date</b>	<b>Changes</b>
1.0.0(Draft)	July 29, 2010	Initial Release.
1.0.0 (Working Final)	August 19, 2010	Updated in response to FDOT comments on Draft.

# 1. Scope

## 1.1 Document Identification

This document serves as the Software Security Plan (SSP) for the SunGuide® Support, Maintenance and Development (SMD) contract. This document describes how Southwest Research Institute® (SwRI®) and its subcontractors will protect the Florida Department of Transportation (FDOT) intellectual property embodied in the SunGuide software. Specifically, it describes the physical and network security.

## 1.2 Project Overview

The FDOT SunGuide Support, Maintenance and Development Contract, contract number BDQ69, addresses the necessity of supporting, maintaining and performing enhancement development efforts to the SunGuide software. The SunGuide software was developed by the FDOT in a contract from October 2003 through June 2010. The SunGuide software is a set of Intelligent Transportation System (ITS) software that allows the control of roadway devices as well as information exchange across a variety of transportation agencies and is deployed throughout the state of Florida. The SunGuide software is based on ITS software available from the state of Texas; with significant customization and development of new software modules to meet the needs of the FDOT. The following figure provides a graphical view of the SunGuide software architecture:

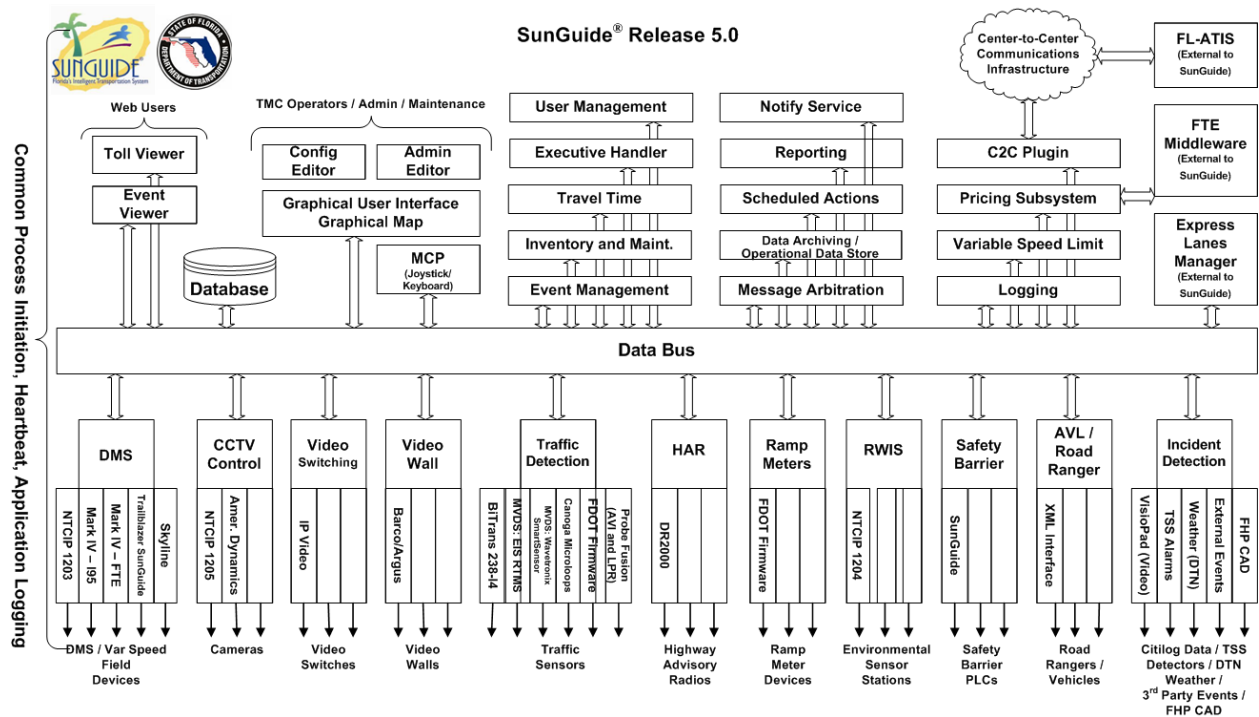


Figure 1-1 – High-Level Architectural Concept

### **1.3 Related Documents**

Additional information regarding the SunGuide project can be found in the following documents and electronic publications:

- FDOT Scope of Services: *BDQ69, Standard Written Agreement for SunGuide Software Support, Maintenance, and Development, Exhibit A: Scope of Services*. July 1, 2010.
- Notice to Proceed: Letter to SwRI for BDQ69, July 1, 2010
- Letter of Authorization 001: Letter to SwRI for BDQ69, July 1, 2010.
- SunGuide Project website: <http://sunguide.datasys.swri.edu>.
- SunGuide SMD Software Development Plan, <http://sunguide.datasys.swri.edu>

### **1.4 Contacts**

The following are contact persons for the SunGuide software project:

- Elizabeth Birriel, ITS Section, Traffic Engineering and Operations Office, [elizabeth.birriel@dot.state.fl.us](mailto:elizabeth.birriel@dot.state.fl.us), 850-410-5606
- Arun Krishnamurthy, FDOT SunGuide Project Manager, [Arun.Krishnamurthy@dot.state.fl.us](mailto:Arun.Krishnamurthy@dot.state.fl.us), 850-410-5615
- Khue Ngo, PBS&J Project Manager, [khue.ngo@dot.state.fl.us](mailto:khue.ngo@dot.state.fl.us), 850-410-5579.
- David Chang, PBS&J Project Advisor, [David.Chang@dot.state.fl.us](mailto:David.Chang@dot.state.fl.us), 850-410-5622
- Robert Heller, SwRI Project Manager, [rheller@swri.org](mailto:rheller@swri.org), 210-522-3824
- Tucker Brown, SwRI Software Project Manager, [tbrown@swri.com](mailto:tbrown@swri.com), 210-522-3035

## **2. SunGuide Source Code Protection**

The SunGuide source code embodies intellectual property owned by the FDOT and the TxDOT. The SunGuide source code has been delivered to the FDOT at various times during its development. The FDOT has subsequently provided the SunGuide source code to at least one district (District 4) who has provided that source code to another software developer. This document does not address the protection of the FDOT and TxDOT intellectual property by organizations other than SwRI.

### **2.1 SwRI Source Code Storage**

SwRI stores the SunGuide source code in five forms:

1. In an electronic source code repository at the SwRI site at 6220 Culebra Road in San Antonio, Texas in Building 68,
2. Backup tapes of the repository (see section 2.3.7) at the SwRI site at 6220 Culebra Road in San Antonio, Texas in Building 68,
3. SwRI employees may keep copies of source code they are actively modifying or creating on development computers,
4. SwRI employees may keep copies of source code they are actively modifying or creating on laptop computers,
5. Copies of delivery media

Employees of Lucent Group providing on-site support to the FDOT will have the same access to the SunGuide source code as SwRI on-site support employees and will be required to obey the same restrictions as SwRI employees.

#### *2.1.1 Source Code Repository*

The SunGuide source code is stored in a password protected AccuRev database. SwRI provides user accounts and passwords to the AccuRev database only to those staff members authorized to work on the SunGuide project. If a team member leaves the project, their account is removed from the AccuRev list of users. The AccuRev source code repository is accessible from the SwRI Division 10 network; network security is discussed later in this document.

#### *2.1.2 Desktop Security*

SwRI employees may store working copies of selected portions of the SunGuide source code on their desktop workstations which they are actively modifying or creating. The desktop workstations are members of the ADS<sup>1</sup> domain and are username/password protected; password strength rules that are described later apply. Desktop computers are also subject to the physical security rules that are described later.

#### *2.1.3 Laptop Security*

SwRI employees may store working copies of selected portions of the SunGuide source code on their SwRI supplied laptops which they are actively modifying or creating. The laptops are members of the ADS domain and are username/password protected; password strength rules that are described later apply. While in the SwRI facilities these laptops are subject to the physical

---

<sup>1</sup> ADS is a Microsoft Windows Domain name utilized by the Automation and Data Systems (ADS) Division (aka Division 10) at SwRI. The SunGuide SMD project is managed within the SwRI Division 10 organization.



security rules that are described later. While not in SwRI facilities, employees are responsible for the security and protection of the laptops and their contents. Recognizing the physical vulnerability of the laptops and their disks, SwRI Division 10 support staff have embarked on a trial program to encrypt laptop disks to further protect their contents. Pending the success of this trial program the requirement to encrypt laptop disks will be extended to all Division 10 laptops.

### *2.1.4 Copies of Delivery Media*

SwRI maintains copies of all media delivered to the FDOT, i.e. SwRI maintains file copies of optical media (Digital Versatile Disks [DVD] and Compact Disks [CD]) containing the source code that SwRI has delivered to the FDOT. SwRI maintains copies of these media in file cabinets that are secured within the SwRI Building 68.

## **2.2 Physical Security**

SwRI takes the security of the SunGuide software very seriously. As such, SwRI has policies in place to ensure that the location where the software is stored is physically secured.

### *2.2.1 Campus Security*

SwRI's San Antonio campus has an "open campus" policy between the hours of 7AM to 6PM CT. Between the hours of 6PM and 7AM CT SwRI contracts security officers, whose primary function during SwRI nonworking hours, is to safeguard SwRI property and personnel. During normal working hours, a roving security officer is available. The officer's primary responsibility is to assist visitors and to serve as a visible deterrent to individuals that have no legitimate business at SwRI. As a deterrent to the unauthorized removal of classified material or SwRI property, all personnel and the property under their control, are subject to search while on SwRI grounds.

Blue SwRI identification badges must always be worn by employees while on SwRI grounds, unless wearing the badge poses a threat to employee safety. In addition to identification badges, vehicles routinely driven on SwRI grounds by regular employees must be registered with the Human Resources Department and are required to display a sticker on their vehicles as proof of registration.

A guard at the main gate will be required to view the SwRI vehicle sticker or the employee's SwRI blue photo identification badge and log the employee's number during times other than normal business hours or periods of increased security.

### *2.2.2 Building Security*

Physical security at SwRI for each building is managed by the individual technical division(s) whose staff or equipment occupies the building. Identification badges for Division 10 are programmable to allow access to certain parts of the facilities. Every Division 10 staff member has an individual profile that can be tailored to allow access to only the area to which they are authorized to enter. These profiles are only accessible to the Division 10 Network Support Group and can only be changed with specialized hardware and software.

For the purposes of this contract, Division 10's Building 68 will be used exclusively. Building 68 locks all exterior doors, at all times, except the lobby entrance, which is unlocked between the hours of 8AM to 5PM CT on weekdays. During this timeframe, the lobby entrance is physically monitored by a Division 10 staff member. Access to exterior doors is granted to all Division 10 staff members at all times, through the use of their identification badge. Visitors who do not have

badge access, may use the lobby entrance and check in with the receptionist. Visitors will be issued temporary badges and must be escorted at all times by a Division 10 employee.

### 2.2.3 Lab Security

Development labs for the SunGuide Project share a lab with developers working on ATMS systems for TxDOT. Only developers and management staff working these projects have access to the lab space. Each developer is responsible for maintaining their workstation in the lab. Each workstation requires that users enter a username/password in order to log on to the system. The password policy is located in section 2.3.6. Occasionally, laptops are also used by developers but are subject to the same rules about password access as workstations.

### 2.2.4 Server Security

Servers running the SunGuide software are maintained in a separate server room, away from the lab space. This room restricts access to only those who need access to the sever room. This access is maintained by the Division 10 Network Support Group. For information on the backup policy for servers, please go to section 2.3.7.

## 2.3 Network Security

Network Security is controlled by the SwRI Division 10 Support Staff. The following sections detail the Network Security Policy implemented and enforced by the support staff.

### 2.3.1 Network Topology

The design goals for the network topology include protecting the intellectual property of the SwRI and the SwRI's clients while providing a means by which project requirements can be met. Figure 2-1 presents a logical overview of network topology for the SwRI Division 10 Network.

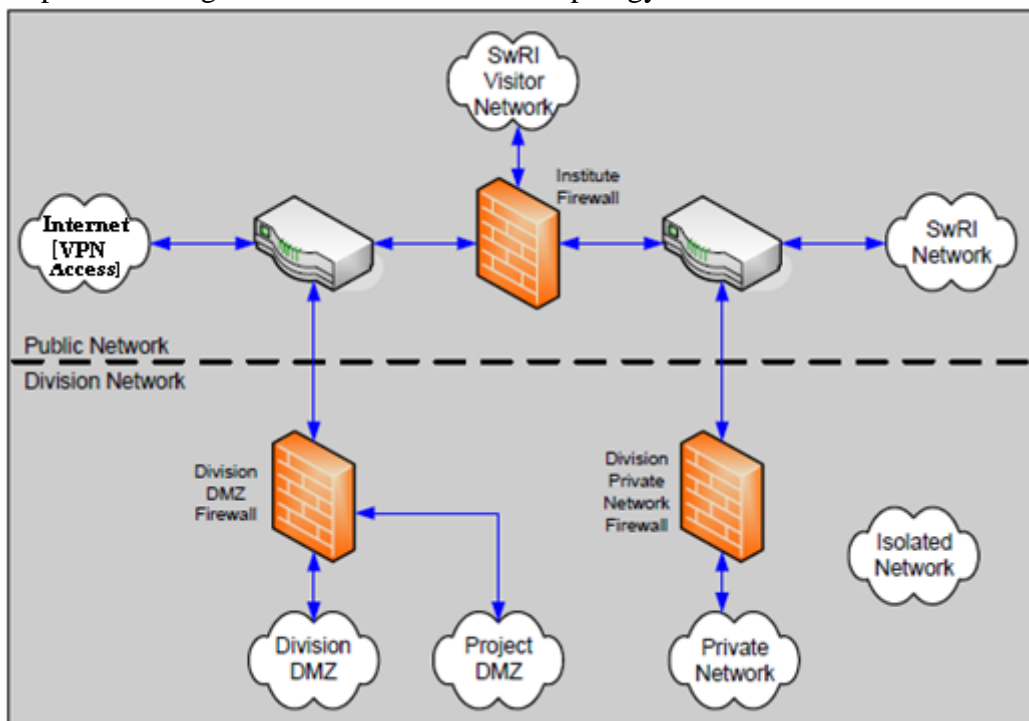


Figure 2-1 – Logical View of the SwRI Division 10 Network

The Division 10 Private Network is protected by the Division 10 Private Network Firewall that is, by default, configured to allow most outgoing connections and disallow all incoming connections.

The Division and Project DMZs (De-Militarized Zones) provide network regions where selected project and Division networked assets can be placed so as to be accessible from the public network without the need for a VPN. All connections to and from the Division and Project DMZs are configured on the Division DMZ Firewall on an as-needed basis and are documented in an approved Division 10 DMZ Authorization Form (Attachment B).

Isolated Networks provide projects the ability to network resources without Private or Public Network access.

The SwRI Visitor Network is provided in various conference rooms throughout Division 10. The SwRI Visitor Network provides outbound network connectivity for clients and visitors while still protecting the Division 10 Network and the SwRI Network.

### *2.3.2 Network Access Rules*

This section describes the rules affecting network-to-network connectivity within the Division 10 network.

#### *2.3.2.1 Public Network to Private Network*

Access from a single computer on the Public Network to the Private Network shall be allowed only via the Division 10 approved VPN. Access from the Public Network to the Private Network without the use of the Division 10 approved VPN may be approved on a case-by-case basis and requires an approved Division 10 Network Security Policy Waiver Form (Attachment C).

#### *2.3.2.2 Private Network to Public Network*

Access from the Private Network to the Public Network shall be on a case-by-case basis in the event of a network emergency (such as a virus outbreak) as determined by the Division 10 Network Administrator. Outbound traffic from the Private Network may be filtered by the SwRI Information Technology Center (ITC) based on protocol and/or content.

#### *2.3.2.3 DMZ to/from Other Networks*

Access to and from the DMZ shall be restricted to only the necessary protocols and/or services as documented on an approved Division 10 DMZ Authorization Form.

### *2.3.3 Physical Access*

This section describes the physical access rules to the defined networks controlled by Division 10. Physical access in this context refers to wired and wireless connectivity to a Division 10 network resource and to devices connected to a Division 10 controlled network resource.

### *2.3.3.1 Physical Access to the Private Network*

The Division 10 Network Support Group shall grant authorization for approved network hardware that connects logically or physically to the Private Network. Network hardware includes, but is not limited to, infrastructure wiring, hubs, switches, routers, firewalls, modems, and wireless access points. Network cables connecting computers to the network wall plates are not included. All private computers connecting to the private network must be coordinated with Division 10 Network Support Group.

Only SwRI-owned equipment, Government Furnished Equipment<sup>2</sup> (GFE), or Client Furnished Equipment<sup>3</sup> (CFE) shall be connected to the Division 10 Private Network (i.e. consultant owned and personal equipment may not be connected to the Private Network). Client-owned equipment (e.g. laptops) used by the client during visits to SwRI are not considered to be GFE or CFE. SwRI Employees not in Division 10 and SwRI Consultants may have access to the Private Network only for the purpose of conducting or supporting Division 10 business. A completed and approved Division 10 Account Request Form (Attachment A) shall be required to document the need for such access. Non-Division 10 SwRI Employee and Consultant accounts shall be reviewed annually and at the end of assigned project activities. Non-Division 10 SwRI Employee and Consultant accounts shall be disabled if no longer justified.

Clients and/or subcontractors shall be allowed supervised use of their CFE/GFE on the Private Network. The Project Manager shall be responsible for ensuring that clients are supervised at all times while utilizing CFE/GFE on the Private Network. Supervision in this context means that a Division 10 Employee shall visually monitor the client at all times while they are utilizing the Private Network. Equipment (SwRI-owned, GFE, and/or CFE) used by clients and/or subcontractors shall be configured to restrict user access to the Private Network and local machine (using non administrative local accounts). GFE and CFE shall be evaluated by the Division 10 Network Support Group prior to connecting the equipment to the Private Network to ensure the equipment meets the minimum requirements for software patches and anti-virus protection prior to connection of the equipment to the Private Network. The Division 10 Network Support Group shall periodically scan the ports of GFE/CFE equipment connected to the Private Network for known vulnerabilities.

Vendors shall connect their equipment to the Private network only with an approved Division 10 Network Security Policy Waiver Form. Vendors shall only be provided supervised access while using their equipment on the Private Network. The SwRI Point of Contact shall be responsible for ensuring that vendors are supervised, at all times, while utilizing the Private Network. Supervision, in this context, means that a Division 10 Employee shall visually monitor the vendor, at all times, while they are utilizing the Private Network.

Division 10-provided laptops shall be allowed to connect to the Private Network after being connected to the Public Network. The intent of this rule is to allow Division 10-provided laptops to be used by Division 10 employees while away from the SwRI, for example, while on travel and at home. All equipment connected to the Private Network shall utilize the Division 10

---

<sup>2</sup> Government Furnished Equipment (GFE): equipment provided by a government client to be used exclusively by SwRI personnel for the duration of the project to complete project deliverables.

<sup>3</sup> Client Furnished Equipment (CFE): equipment provided by a commercial client to be used exclusively by SwRI personnel for the duration of the project to complete project deliverables.

approved anti-virus solution. If technical limitations prevent the use of the approved antivirus solution, then an approved Division 10 Network Security Policy Waiver Form shall be required to exempt the equipment from this requirement. If exempt, the Project Manager shall be responsible for ensuring that exempted systems are protected from virus outbreaks and do not infect other systems. Exempt systems shall be periodically audited for compliance by the Division 10 Network Support Group. All equipment connected to the Private Network shall have software patches managed by the Network Support Group patch management solution. If technical limitations prevent the use of the approved patch management solution, then an approved Division 10 Network Security Policy Waiver Form shall be required to exempt the equipment from this requirement. If exempt, the Project Manager shall be responsible for ensuring the system is kept up-to-date with regards to software patches. Exempt systems shall be periodically audited for compliance by the Division Network Support Group.

### *2.3.3.2 Physical Access to the Division DMZ*

The Division 10 Network Support Group shall administer all network connections to the Division DMZ. Resources shall be placed in the Division DMZ upon approval of a Division 10 DMZ Authorization Form. All equipment attached to the Division DMZ shall be physically located in the Division DMZ locations designated by the Division 10 Vice President.

Only authorized personnel shall be granted physical access to the Division 10 DMZ. Authorized personnel include the Division 10 Network Support Group and those personnel listed on the relevant Division 10 DMZ Authorization Form. Only Division 10 Authorized Employees shall be provided unsupervised physical access to the Division DMZ locations. Physical access to Division 10 DMZ locations shall be limited to the minimum time necessary to provide installation and/or maintenance of the equipment.

A room containing a Division 10 DMZ shall only have connections to the DMZ within the room. For example, a room with Division 10 DMZ connections cannot have Private Network connections.

General-purpose use of resources in the Division 10 DMZ shall not be allowed. An example of activity considered to be “general purpose” is software code development.

Computer resources located in the Division 10 DMZ may be shared across projects at the discretion of all involved project managers, but each project utilizing a shared resource shall obtain an approved Division 10 DMZ Authorization Form prior to utilizing the shared equipment. The Project Manager shall be identified as the primary point of contact and shall be responsible for the resource.

The Project Manager shall be responsible for ensuring project-related resources located in the Division 10 DMZ are maintained appropriately (for example, operating system patches are kept up to-date) to prevent known vulnerabilities from being exploited. Equipment connected to the Division 10 DMZ may be scanned for security vulnerabilities at the discretion of the Division 10 Network Administrator.

### *2.3.3.3 Physical Access to the SwRI Visitor Network*

Vendors and Clients may connect to the SwRI Visitor Network without supervision. While in Division 10 controlled facilities, Division 10 Employees shall not use the SwRI Visitor Network for conducting regular Division 10 business or for convenience.

### *2.3.3.4 Virtual Private Network (VPN) Access to Private Network*

The Division 10 Network Support Group shall administer Division 10 VPN accounts. Non-Division 10 SwRI Employees may request VPN accounts from the Division 10 Network Support Group. The Division 10 Account Request Form is not necessary for Division 10 Employees. Non-Division 10 SwRI Employees may be provided VPN access provided that such access is required to support Division business. An approved Division 10 Account Request Form shall be required for Non-Division 10 SwRI Employees. Consultants, clients, and vendors shall not be provided VPN access for any reason. Individual VPN account holders shall not share the VPN account with anyone under any circumstance.

### *2.3.3.5 Outbound VPN Access from the Private Network*

Outbound VPN connections to a Public Network from the Private Network shall be allowed only with an approved Division 10 Network Security Policy Waiver Form. Systems with outbound VPN access shall adhere to the same rules defined in the Physical Access to the Private Network section of this document. Systems with outbound VPN access shall provide monthly verification of up-to-date status to the Division 10 Network Support Group.

### *2.3.4 Policy Enforcement*

Network traffic passing through the firewall shall be logged and monitored as necessary at the discretion of the Division 10 Network Administrator to protect Division 10 network security and integrity. The Division Network Administrator has the authority to temporarily terminate any or all services, at any time, to protect Division 10 network security and integrity. Division 10 staff affected by a termination of service shall be notified of the termination by the Network Support Group within a reasonable amount of time depending upon the nature of the issue.

### *2.3.5 Firewall Maintenance*

The Division Network Support Group shall be responsible for the administration of all Division firewalls. The Division Network Support Group shall audit the rule sets implemented on the Division firewalls semi-annually, at a minimum. All rules activated on the Division firewalls shall be documented on an approved Division 10 DMZ Authorization Form or on a Division 10 Network Security Policy Waiver Form.

### *2.3.6 Password Policy*

The following is the standard for Division 10 Passwords:  
The password must:

- have at least 7 character(s)
- not be longer than 12 characters
- have upper and lower case characters

- have no more than 12 upper-case letter(s)
- have no more than 12 lower-case letter(s)
- have a leading letter
- have at least 1 digit(s)
- not be your username
- not be an old password
- have no more than 2 pair(s) of repeating characters
- Must Not Contain “<” or “>” or single quote.

The password should:

- not be constructed from a dictionary word.
- not be an exact dictionary word match.
- not contain a dictionary word.
- not contain an exact dictionary word match.

Passwords are also required to be changed every three months, or access to the workstations will be denied.

### *2.3.7 Server Backup Policy*

Routine backups are performed on all servers to ensure any failure results in as little lost data as possible. The backups are as follows:

- Every Friday a “full” backup is performed. All files in the backup set are backed up. As soon as that job is complete a duplication job is run to create a second copy of the tapes.
- Every Monday through Thursday a “differential” backup is performed. All files changed, as determined by the Archive bit, are backed up. As soon as each job is complete a duplication job is run to create a second copy of the tapes.
- Each backup job starts at 5:00 PM, but only one server at a time is backed up so the time will vary for each of the servers in the list.

Backups created on Monday through Thursday are retained for two weeks. The backup created on the first Friday of the month is retained for two years. The backups created on the other Fridays of the month are retained for 6 weeks.

**Attachment A**  
**Division 10 Account Request Form**







Division 10 Account Request Form



GENERAL INFORMATION			
Application Type:	<input type="checkbox"/> New	<input type="checkbox"/> Update	<input type="checkbox"/> Annual Review
Project Manager:		Department:	
Project Number:		Section:	
ACCOUNT REQUESTED FOR			
First Name:		Employee/Badge #:	
Last Name:		Department/Cost Center:	
Middle Initial:		Office Phone Number:	
Consultant:	<input type="checkbox"/> Yes <input type="checkbox"/> No		
ACCOUNT TYPES REQUESTED (check all that apply)			
Domain Account:	<input type="checkbox"/> Check if an ADS Domain Account is required		
VPN Account:	<input type="checkbox"/> Only available to Institute Employees		
Email Account:	<input type="checkbox"/> Consultant email account will be <username>@consultant.datasys.swri.edu		
File Server Access:	<input type="checkbox"/>	Initial Folder/Share:	
Expiration Date:		Read/Write?	<input type="checkbox"/>
NOTES			
<p><i>This form is not required for Division 10 employees. To request a SwRI Domain or SwRI VPN Account, use the ITC/FDS Account Request Form (IFAR) NOT this form.</i></p>			
APPROVALS			
	Project Manager	Date	
	Director	Date	
FOR DIVISION 10 NSG USE ONLY			
User ID Assigned:		Initial Password:	
Email Alias Assigned:			
Date Validated:		Validated By:	
Annual Review Date:		Annual Review By:	

**Attachment B**  
**Division 10 DMZ Authorization Form**

	<b>Division 10</b>			
<b>DMZ Authorization Form</b>				
<b>GENERAL INFORMATION</b>				
<b>Application Type:</b>	<input type="checkbox"/> New <input type="checkbox"/> Update <input type="checkbox"/> Annual Review	<b>Date:</b>		
<b>Project Manager:</b>		<b>Department:</b>		
<b>Project Number:</b>		<b>Section:</b>		
<b>ITC Waiver Required:</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No <i>Required for DMZ to SwRI Network connections</i>			
<b>Client Name:</b>				
<b>Client Contact:</b>				
<b>Client Address:</b>				
<b>JUSTIFICATION</b>				
<i>Describe the business need for requesting a waiver to the Division 10 Network Security Policy. Convenience is not sufficient justification to warrant a waiver. Please replace this text with your justification.</i>				
<b>ACCESS REQUIREMENTS</b>				
<b>Expiration Date:</b>		<b>Host Name:</b>		
<b>System Administrator:</b>		<b>IP Address:</b>		
<b>Device Description:</b>		<b>OS:</b>		
<b>Shared Resource?</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No	<b>Primary PM:</b> <i>Enter if a shared resource</i>		
<b>DMZ Type:</b>	<input type="checkbox"/> Division <input type="checkbox"/> Project	<b>Location:</b> <i>Enter if Project DMZ</i>		
<b>Room Access (Max 2):</b>				
<i>Send email notification to <a href="mailto:support@datasys.swri.edu">support@datasys.swri.edu</a> for OS and DMZ Room Access changes.</i>				
<b>REQUESTED SERVICES</b>				
<b>ID</b>	<b>Service</b>	<b>From</b>	<b>To</b>	<b>Reason for Access</b>
1				
2				
3				
4				
5				
6				
<b>APPROVALS</b>				
Project Manager		Date		
Recommended				
Yes	No	Rationale	Initials	
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
Director		Date		
<b>Authorization Number:</b>		<b>Renewal Date:</b>		

- The following steps recommended for getting a DMZ Authorization Form completed, routed, and approved:*
- 1. After discussing the project needs with the Network Support Group, fill out this form. Working with the Network Support Group early in the process will help to ensure the information provided in the form is technically accurate and complete prior to routing the form to management for approval.*
  - 2. Submit the completed form signed by the Project Manager to the Network Support Group for approval routing.*

**Attachment C**  
**Division 10 Network Security Policy Waiver**  
**Form**

	<b>Division 10</b>			
<b>Network Security Policy Waiver Form</b>				
<b>GENERAL INFORMATION</b>				
<b>Application Type:</b>	<input type="checkbox"/> New <input type="checkbox"/> Update <input type="checkbox"/> Annual Review	<b>Date:</b>		
<b>Project Manager:</b>		<b>Department:</b>		
<b>Project Number:</b>		<b>Section:</b>		
<b>ITC Waiver Required</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No			
<b>Client Name:</b>				
<b>Client Contact:</b>				
<b>Client Address:</b>				
<b>JUSTIFICATION</b>				
<p><i>Describe the business need for requesting a waiver to the Division 10 Network Security Policy. Convenience is not sufficient justification to warrant a waiver. Please replace this text with your justification.</i></p>				
<b>ACCESS REQUIREMENTS</b>				
<b>Expiration Date:</b>		<b>Host Name:</b>		
<b>System Administrator:</b>		<b>IP Address:</b>		
<b>Location:</b>		<b>OS:</b>		
<b>Description:</b>	<i>For Example: Dell Optiplex Workstation</i>			
<i>Send email to support@datasys.swri.edu for OS changes Location and hardware changes require an updated form.</i>				
<b>REQUESTED SERVICES</b>				
ID	Service	From	To	Reason for Access
1				
2				
3				
4				
5				
6				
7				
<b>APPROVALS</b>				
Project Manager		Date		
<b>Recommended</b>				
Yes	No	Rationale	Initials	
<input type="checkbox"/>	<input type="checkbox"/>		Division Network Administrator (or designee)	
<input type="checkbox"/>	<input type="checkbox"/>		Division Computer Committee Chair (or designee)	
Director		Date		
<b>Authorization Number:</b>		<b>Issue/Renewal Date:</b>		

- The following steps recommended for getting a Network Security Policy Waiver Form completed, routed, and approved:*
- After discussing the project needs with the Network Support Group, fill out this form. Working with the Network Support Group early in the process will help to ensure the information provided in the form is technically accurate and complete prior to routing the form to management for approval.*
  - Submit the completed form signed by the Project Manager to the Network Support Group for approval routing.*