UNCLASSIFIED

Rules of Behavior
Department of State SharePoint System (DOSSS)
Internet DMZ

Version 1.0

January 30, 2012

Prepared By:

United States Department of State
IRM
Information Resource Management

Systems & Integration Office (SIO)

IRM/OPS/SIO/CCS

SIO
Collaboration and Compensation Services

Author:	E. Foreman
Distribution:	This document is for U.S. Department of State, IRM/OPS/SIO/CCS *Internal Use Only*.
Document Location:	The master copy of this document resides at: *\\siomossmgt01\ecs-share\Master Documents\Agreements\DMZ Rules of Behavior.docx*

Document History

Date	Version	Sections/Pages Affected	Comments
02/25/2011	0.1	All	Initial Draft
04/19/2011	0.2	All	Draft 2
06/29/2011	0.3	All	Clarifying roles, removing PII info
10/06/2011	0.4	All	Adding in info from Privacy group re: PII
01/30/2012	1.0	All	Final review

Table of Contents

Section 1.0 Introduction

The Office of Management and Budget (OMB) Circular A-130, Appendix III Security of Federal Automated Information Resources requires that "Rules of Behavior" be established for each general support information technology system and major application processing government information. The Rules of Behavior delineated below pertain to all persons who utilize the Department of State SharePoint Services (DOSSS) web portal, which is an IT resource for the Department of State (DoS). The following Rules of Behavior and acceptable use policy apply to all administrators and contributors in the DOSSS environment whether they are DoS employees, contractors, or members of external agencies.

The Rules of Behavior provide general instructions on the appropriate use of the DOSSS and specifically apply to SharePoint sites and their respective sub-sites in the Internet Demilitarized Zone (DMZ)[1].

Section 2.0 SharePoint Overview

SharePoint allows you to:

- Store your organization's documents and information securely
- Collaborate on documents and reports
- Manage content and streamline processes
- Build a collaboration and published website for information sharing and or marketing purposes
- Search for documents and sites

[1] DOSSS in the Internet DMZ is referred to internally as "DOSSS-I."

Section 3.0 User Access

3.1 Upon initial login to Internet DMZ, users will be required to change their initial assigned passwords to new, unique passwords. Users will be required to change their passwords every 180 days thereafter. This policy is subject to change per the requirements of the Active Directory team.

3.2 The Internet DMZ Administrator will be responsible for verifying and creating accounts for site users.

3.3 The Internet DMZ Administrator will be responsible for reviewing all user accounts to determine whether the accounts and/or levels of access granted by the accounts are still required.

3.3.1 User accounts will be disabled when the following events occur:

- The user requests account termination
- A discretionary termination request is received from the DoS Authorized POC
- A discretionary termination request is received from the Internet DMZ Administrator
- The account has been abandoned (i.e., the account is inactive for more than 180 days)
- The user separates from their Requesting User's Organization (RUO) (subject to confirmation)
- The user violates the DOSSS Rules of Behavior for the Internet DMZ.

3.3.2 The Requesting User's Organization (RUO) POC must inform SIO immediately when a user no longer needs their account due to change of duties, transfer, separation, or other cause.

3.3.3 The request to terminate the account must be submitted to the ITSC by the Internet DMZ Administrator along with the user's username, full name and email address and the contact information for the DoS Authorized POC and Internet DMZ Administrator.

3.3.4 Upon receipt of the account termination request from the Internet DMZ Administrator, the SIO representative will delete (not disable) the user's account from the APP domain

Active Directory. ITSC will send an account termination notification to the Internet DMZ Administrator and DoS Authorized POC once the account has been deleted.

Section 4.0 Data Classification and Security

4.1 All Internet DMZ users have an obligation to safeguard information with national security and/or privacy implications.

4.2 Internet DMZ sites residing on or accessible via the Internet DMZ network are for the processing of Unclassified data only.

4.3 Each DoS page will display an appropriate classification banner informing the user of the page's security classification as determined by the System Categorization Form by Information Assurance (IA). Internet DMZ users will take note of the classification and treat the data on the page accordingly.

4.4 The Administrator will periodically review the site to ensure that no data higher than the approved classification level is posted.

4.5 The Administrator will ensure that Contributors are familiar with these data classification and security rules of behavior and that every effort is made to prevent "data spillage."

4.6 If an Internet DMZ user observes content that is a higher classification level than approved, they must immediately report this infraction to the Administrator.

4.6.1 The Administrator receiving the report will immediately remove the prohibited content from the affected site.

4.6.2 The Administrator will then report the infraction to their ISSO, who will instruct the ITSC on how to proceed. The Administrator will also notify SIO via Remedy ticket. The standard response will be to remove any prohibited content from all site back-ups and locations as needed.

Section 5.0 User Permissions

5.1 All SharePoint users within the DMZ are assigned a permission level that provides them access privileges and functional capabilities appropriate to their business functions. In general, users are granted the lowest permission level necessary for them to carry out their jobs. These permission levels form the basis for creating custom user groups. The following SharePoint site permission levels will be available to Internet DMZ users:

- **Readers (General Users)**—A Reader of a site has the ability to read items and content to which they have read access. A Reader is designated a Reader of the site by the Site Administrator.
- **Contributors (Users)—A** Contributor is an individual who adds (posts), deletes, and edits content on a collaboration site. An individual is assigned Contributor permissions by the Site Administrator, based on a business need to exercise Contributor permissions on the site. Contributor permissions are granted only after the individual has read and agreed to the MOSS Rules of Behavior for the network on which their site resides.
- **Designers (Power Users)**—Designers plan the site's physical layout and information architecture, perform updates and customizations to the site, and generally monitor and maintain its validity and usability.
- **Site Administrators (Full Control)**—Site Administrators are responsible for performing the software procedures that govern the configuration of the site interface and users' access to the site. Site Administrators also ensure that site participants can use the site by providing training, complying with usability and accessibility standards, etc. As a best practice, at least two Site Administrators manage each SharePoint site and its sub sites to ensure proper management and control of administrative functions.

5.2 Only cleared DOS users are eligible to be Site Administrators and they must meet all SCA requirements

5.2.1 Only cleared US Government users (example: .mil or.gov email addresses) are eligible for Designer permissions on Unclassified sites.

5.2.2 Cleared non-DoS users are eligible for Contributor or Reader permissions.

5.2.3 Only cleared, authorized DoS administrative users will be able to access Internet DMZ administrative functions, application back ends, or databases from the DMZ.

5.2.4 All permission groups must be assigned. Under no circumstances should all authenticated users be able to access all information.

5.3 Only users provided with access to specific content (e.g., lists, individual files) will be able to view them. The existence of content, data, and applications will be hidden from other SharePoint users not authorized to see them.

5.4 Internet DMZ Administrator will be responsible for defining granular levels of site access based on who a user is, the groups to which the user belongs, and the degree to which that user is compliant with corporate governance policy.

5.5 The Internet DMZ Administrator will be responsible for managing permissions on their sites. The Access Request function must be enabled at the Site level. This ensures that users who wish to access the site, sub-sites, or specific content items will have someone follow-up with them and either grant or deny them rights to the site.

Section 6.0 SharePoint Rules of Behavior

6.1 The Rules of Behavior are suggested guidelines and best practices for using SharePoint in the DOS environment regardless of the site classification level.

6.2 New Internet site requests require approval of the site's system categorization by the Bureau of Information Assurance (IA). The SharePoint Internet site collection content level will be determined by the categorization level determined by IA. Prior to requesting an Internet site, users must complete a Systems Categorization Form (SCF) and e-Authorization Form.

6.3 Site Administrators, Designers, and Contributors must follow a configuration management process for storing information and data on SharePoint sites.

6.4 Site Administrators are responsible for the management of site content at the top-level site and at the sub-site levels. Sub-sites must meet the same DoS access and data security standards as higher-level sites. Site Administrators may re-assign the responsibility of Content Manager to those individuals who manage particular sub-sites.

6.5 Users who violate the Rules of Behavior must be reported to their local ISSO.

Section 7.0 Non-Acceptable Use – Low DMZ

This policy identifies actions that should not be performed with SharePoint on the Low Internet DMZ.

7.1 It is strictly prohibited to post, review, process, or modify any content above the appropriate content categorization level, any content containing information above the accreditation level, must be recertified by IA.

7.2 Users cannot post combinations of key privacy information or combinations of Personally Identifiable Information (PII) on the Low Internet (DMZ).

7.2.1 These combinations could include but are not limited to full name, birth date, social security number, address, and DoS employees' personnel records.

7.2.2 Examples of personnel records include compensation, rewards, reviews, or appraisals.

7.3 Users should not post items that will affect the National Security of the Department of State or any collaborating agencies.

7.3.1 Examples of non-acceptable information include: Social Security Number + Last Name (or any combination of SSN with other PII, i.e. date of birth, phone number, and first name)

7.3.2 Communications, contracts, or negotiations regarding external affairs

7.3.3 Architectural drawings or floor plans related to DoS facility (embassies, consulates, posts, etc.)

7.4 SharePoint should not be used to post inappropriate documentation, announcements, lists, etc. that could be considered offensive by other site participants.

7.5 Under no circumstances will more than one user be assigned or permitted to use the same user ID and password. Group user IDs and passwords are prohibited.

7.6 Internet DMZ user accounts/login credentials may not be transferred from one user to another.

7.7 The RUO may not request or maintain permanent Internet DMZ user accounts for visitors, vendor service personnel, training, demonstrations, or other purposes.

7.8 Internet DMZ users may not use personal, non-Government email accounts associated with user account (e.g., Gmail, Yahoo, other service provider accounts) to communicate with the Internet DMZ website. Only valid U.S. Government-issued email accounts will be recognized (e.g., .gov, .mil, etc.).

Section 8.0 Use of PII – Moderate DMZ

Rules of behavior regarding the use of PII on the Moderate DMZ are not intended to replace existing policies or guidelines. Rather, they are intended to supplement the present document (*DOSSS Rules of Behavior for Internet DMZ)*. The Moderate DMZ will also comply with the *SIO SharePoint User Governance Model and Standards*, which define the regulations governing the Department of State's SharePoint deployment and usage centrally and regionally. Moderate sites must be approved at the moderate categorization level.

8.1 Users can post combinations of key privacy information or combinations of Personally Identifiable Information (PII) on the Moderate Internet (DMZ) when deemed necessary.

8.1.1 If Personally Identifiable Information (PII) needs to be posted on DMZ please consult the Privacy Division, at Privacy@state.gov, for appropriate guidance on your particular need to collect, maintain, and use PII on your site. Such consultation may include the need to conduct a privacy impact assessment in accordance with the E-Government Act of 2002.

8.1.2 These combinations could include full name, birth date, social security number, address, and DoS employees' personnel records.

Examples of personnel records include compensation, rewards, reviews, or appraisals.

Section 9.0 Other Policies and Procedures

The Rules of Behavior are not to be used in place of existing policy or guidelines. Rather, they are intended to supplement the DoS Information Security Program Policy and the DoS

Information Security Program Handbook. Because written guidance cannot cover every contingency, Department staff are asked to augment these rules and use their best judgment and highest ethical standards to guide their actions.

As with any DoS website, users must adhere to the following guidelines: 5FAH-8 H-100, 5FAH-8 H-200, 5FAH-8 H-400, 5FAH-8 H-430, 5FAH-8 H450, 5FAM-770, and 5FAM-790.

Additionally, for Internet-hosted sites, users must adhere to the Department's guidelines on the clearance and dissemination of information intended for the public, which are provided in 3FAM-4170 and 10FAM-120.

The referenced FAM and FAH documents are available to Internet users at http://www.state.gov/m/a/dir/regs/index.htm.

Appendix A. Glossary

DMZ—De-Militarized Zone. A physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. A DMZ adds an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

DOSSS—Department of State SharePoint Services. The Department's implementation of Microsoft Office SharePoint Services (MOSS) 2007.

IA—Bureau of Information Assurance.

Internet DMZ Administrators - Administrative authority, responsible for approving and creating central accounts and having full control for all sites and subsites in the Internet DMZ.

IT Service Center (ITSC)—Manages Universal Trouble Tickets (UTT) and/or Remedy. The ITSC will be the first line of support for all SharePoint—related issues.

Requesting User's Organization (RUO)—Organization sponsoring non-DoS personnel as Internet DMZ users; e.g., the U.S. Department of Defense.

Sensitive But Unclassified (SBU)—A designation of information in the United States Federal Government that, though unclassified, often requires strict controls over its distribution.

Site Collection Administrators (SCAs)—DOSSS users with highest Administrative authority, responsible for approving and creating central accounts and having full control for all sites and subsites.