
RULES OF BEHAVIOR FOR PRISM

For



**DISTRICT OF COLUMBIA
PRETRIAL SERVICES AGENCY (PSA)**

February 2005

AUTHORS

This document was prepared by:

BearingPoint, Inc.
1676 International Drive
McLean, VA 22102

Version	Change Comments	Date	Author
1.0	Initial Draft	01/21/2005	P. Fields
1.1	Included comments from D. Caravantes	02/14/2005	P. Fields
1.2	Included Incident Response requirements	02/23/2005	P. Fields
1.3	Updated email address	08/13/2007	D. Caravantes

Table of Contents

1. Introduction	4
2. Physical Security.....	5
3. Computer System Responsibilities	6
3.1. Passwords and Computer Access	6
3.2. Confidential Information	6
3.3. Technical.....	7
3.4. Email and Internet Access.....	7
3.4.1. Avoiding Fraudulent Attempts to Learn User Names and Passwords	8
3.5. Work at Home/Remote Access	8
3.6. Protection of Software Copyright Licenses.....	8
3.7. Incident Response Requirements	9
4. Unofficial Use of Government Equipment and Services	10
5. PRISM Rules of Behavior User Agreement.....	11
Appendix A – Suspicious Executable File Types	12

1. INTRODUCTION

The purpose of this document is to establish the Rules of Behavior for PRISM. Rules of Behavior establish standards that recognize knowledgeable users are the foundation of a successful security plan. These rules clearly define standards of behavior for all PSA personnel who access PRISM, including full and part-time Federal employees, contractors, interns and other users. Non-compliance with these rules will result in sanctions equal to the level of infraction.

As described in Policy Statement # 5500, the *PSA Global Information Technology Security Policy* sanctions are compliant with those authorized by the US Office of Personnel Management (OPM) and may range from a written or verbal warning, removal of system access for a specific time period, reassignment to other duties, or dismissal, depending on the severity of the violation. PSA will enforce the use of penalties against any user who willfully violates any PSA or Federal system security (and related) policy as appropriate. Users are also responsible for reporting security incidents, or any incidents of suspected fraud, waste, or misuse of PSA systems to the Branch Manager or his or her designee, who is responsible for reporting the incident to the PSA Office of Information Technology.

The rules set forth in this document are not to be used in place of existing policy; rather they are intended to further delineate and highlight the specific rules each user must follow while accessing and using PRISM. As a supplement, these PRISM Rules of Behavior are consistent with the policy, procedures and rules described in the following official materials:

- PSA IT Security Policies, Management Instructions, and IT Plans available at <http://psainfoweb/itsecurity/>
- The PRISM System Security Plan (SSP), which complies with Federal Regulation, identifies the specific security requirements of the system and interconnected systems, as well as for personnel including management, development personnel, support personnel, and users.
- The Federal Information Security Act of 2002 (FISMA)

2. PHYSICAL SECURITY

Physical security focuses on protecting and limiting access to the office facilities and the computer room facility for PSA. Office and computer room facilities contain important information assets; it is important that unauthorized persons do not have access to these facilities.

All full and part-time PSA employees, contractors and interns must practice the following Rules:

- Keep all proxy cards, badges, access codes, and keys under personal protection.
- Wear your assigned identification and proxy card badges at all times while in the office/building.
- Do not lend your pass or ID badge to anyone.
- If your proxy card or ID badge is lost or stolen, report it immediately to:
 - o The PSA IT Help Desk, Ext. 7930 and
 - o The Security Office, Ext. 7912 or 7956
- Ensure that defendants and visitors have signed the appropriate visitor log and are escorted at all times.
- Never allow any individual who does not have proper identification access to the office space.
- Stop and question any individual who does not have proper identification, and contact the Security Office, Ext. 7912 or 7956 immediately for assistance to remove an intruder. Seek the support and cooperation of co-workers as appropriate.
- Maintain control over your PSA provided hardware/software to prevent theft, unauthorized use/disclosure, misuse, denial-of-service, destruction/alteration of data, or violation of Privacy Act restrictions.
- When not in use, keep your desk clear to ensure that sensitive and confidential information is properly secured.

3. COMPUTER SYSTEM RESPONSIBILITIES

Computer system responsibilities focus on the security of software and applications. Users must address these responsibilities when using PRISM to prevent potential threats of compromise to the system. For example, installing computer programs of unknown origin can introduce security vulnerabilities due to questionable or malicious coding and therefore is prohibited. Documents and PRISM printouts must be properly handled, stored or disposed of to ensure sensitive and confidential information does not remain in sight for unauthorized individuals to see and possibly exploit. The misuse of PRISM and the weakening of its security controls could compromise the integrity of PRISM data, adversely impact the system function, and in turn be highly detrimental to the PSA mission.

3.1. Passwords and Computer Access

Users are responsible for safeguarding and maintaining their PRISM passwords and workstations in accordance with the rules below:

- Only use PRISM software and data for which you have an expressed authorization and use them for authorized purposes only. In accordance with the Confidentiality Agreement that all PSA employees sign during training, no employee is permitted to look up anyone in PRISM with whom they might have a personal or professional relationship or acquaintance. If there is doubt about whether or not you may query information about an individual, seek guidance from your supervisor or branch manager before proceeding.
- The password must be 8 characters long and include at least a number or a special character.
- Your password must be changed at least every 90 days.
- Do not share your password with anyone.
- Memorize your password and do not write it down.
- Do not allow anyone else access to your machine when you are logged in
- When you step away from your workstation, make sure that you either log out, or lock the screen so that nobody else can access your computer.
- Protect confidential and/or sensitive information from disclosure.
 - Keep your computer screen turned away from defendants and others who do not have authorized access.
- Do not store data on your individual workstation.

3.2. Confidential Information

- Make sure PRISM generated reports that contain sensitive and confidential data have a cover sheet.
- Shred hard copies of PRISM generated reports or defendant information that is not going to file.
- When faxing always use a cover sheet with the following legal disclaimer:

The information in this fax is confidential and may be legally privileged. Access to this fax by anyone other than the intended addressee is unauthorized. If you are not the intended recipient of this message, any review, disclosure, copying, distribution, retention, or any action taken or

omitted to be taken in reliance on it is prohibited and may be unlawful. If you are not the intended recipient, please destroy the fax message, any attachments, and any copies thereof.

- Do not fax confidential or potentially sensitive information to an unattended fax machine.
- Always check the destination fax number before starting your transmission.
- Do not leave messages containing sensitive or confidential information on answering machines and voicemail.

3.3. Technical

- Do not install hardware or software without authorization the PSA Office of Information Technology.
- Do not, without specific authorization, read, alter, or delete any other person's computer files or e-mail, even if the operating system of the computer allows you to do so.
- Unless otherwise expressly authorized, do not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system.
- Do not write or put into production any "back door" means of accessing the system or applications.
 - Reminder: Any user found to introduce malicious software, coding, programs, or scripts, is subject to prosecution under local, state, and federal law and is subject to local department policies, which enforce disciplinary action up to, and including dismissal.
- Users should never attempt to circumvent any security measures for software applications.
- Do not make copies of system configuration files for your own use, unauthorized use, or to provide to others for unauthorized use.
- Highly sensitive information stored on removable media should be entirely erased, or the disks destroyed. When disposing of, or transferring a computer system, erase all files from the hard drive by using a wipe out utility, or physically destroy the disk if necessary.

3.4. Email and Internet Access

Email and downloading software from unknown sources are often conduits for viruses and other malicious code that can compromise the PRISM system. The following are rules that must be followed to ensure that business and mission critical systems are not exposed to malicious software.

- Employees, contractors and interns must use the same caution with Internet email (such as AOL, CompuServe, Gmail, Netscape, Hotmail, Yahoo, other WebMail, etc.) that they would with PSA email. Any suspicious personal emails must be deleted without opening any related attachments.
- Do not to expose PRISM to viruses by navigating to sites or clicking links that could contain malicious code.
- Do not put sensitive or confidential information into email unless authorized to do so.

- Do not send anonymous messages.
- Do not download or allow to be downloaded (select “no” when prompted), suspicious executable file types (see suspicious file type list in Appendix A) from the Public Internet
- Use the approved anti-virus software on your workstation as recommended by the PSA Office of Information Technology. Do not disable the standard PSA anti-virus software that is on your desktop.

3.4.1. *Avoiding Fraudulent Attempts to Learn User Names and Passwords*

Fraudulent attempts to gain identification and authentication credentials (usernames and passwords) can be made through impersonation. This is called “Phishing”. Messages sent via email or available on web pages, represented as official or best practices may instruct you to input your credentials into form fields. These are captured and used for malicious purposes. Purported assessment of your security posture, offers for free security software and consulting services are also common.

- Do not accept any form of assistance to improve the security of your computer without first having the provider of this assistance approved by the PSA Office of Information Technology.
- Do not accept any offers of free consulting services.
- Do not download any free security software via the Internet.
- Do not engage free security posture evaluation web pages.
- If you are unsure of the source of an expected security related instruction, contact the PSA IT Help Desk, Ext. 7930, or PSA.Helpdesk@psa.gov to verify the source and validate the instruction before proceeding.

3.5. Work at Home/Remote Access

- Remote Access is permitted only for persons who have formal (written) authorization from the PSA Office of Information Technology.
- Remote Access is permitted only for checking work related email.
- Remember that any access to the system, even via remote means, may leave an audit trail.

3.6. Protection of Software Copyright Licenses

- Users must take care to use only software for which they have a license. Do not use software for which you do not have a license.
- Adhere to all purchased software copyright, duplication requirements, and license agreements that are imposed by the vendor. Violations place the individual and PSA at risk of legal action.
- No cost software or “freeware” is permitted as long as it is permissible to use it for work or government (not individual) purposes, and it has been approved by the PSA Office of Information Technology. The PSA Office of Information Technology must approved all freeware downloads.

3.7. Incident Response Requirements

Users must report security problems, suspicious events, and any incidents to the PSA IT Help Desk, Ext. 7930, or PSA.Helpdesk@psa.gov in addition to their direct supervisor.

These incidents include but are not limited to:

- Viruses
- Password security breaches
- Physical security breaches
- Detection of malicious code or software programs, or
- Violations of these rules of behavior.

4. UNOFFICIAL USE OF GOVERNMENT EQUIPMENT AND SERVICES

Employees, contractors and interns are permitted limited personal use of PSA IT resources as long as this personal use does not result in the loss of employee productivity, interference with official duties or other than “minimal additional expense” to PSA.

Unauthorized or inappropriate use of PSA IT resources may result in: 1) loss of use or limitations on use of equipment, 2) disciplinary or adverse actions, 3) criminal penalties and/or 4) employees or other users being held financially liable for the cost of inappropriate use.

- Misuse or inappropriate use of PSA IT resources includes using PRISM for other than need to know for business purposes.
- Remember that access to PRISM may leave an audit trail.
- Any personal use that could cause congestion, delay or disruption of service to any PSA IT resource. For example, greeting cards, video, sound or other large file attachments, and audio and video streaming can degrade network performance.
- The intentional creation, downloading, viewing, storage, copying or transmission of sexually-explicit/oriented materials, or materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or otherwise prohibited activities
- Do not utilize government resources for commercial activity, or any venture related to personal profit or gain.
- Do not utilize government resources for behaviors that are unethical or unacceptable for the work environment, such as improper usage of funds or purchasing equipment without proper approval.
- Engaging in any outside fundraising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity or engaging in any prohibited partisan political activity
- Posting PSA or personal information to external newsgroups, bulletin boards, or other public forums without authority, including information that is at odds with PSA’s mission or positions.
- These Rules of Behavior concerning the use of government equipment and services must be followed in addition to PSA policies concerning standards of employee conduct and personal use of IT resources.

5. PRISM RULES OF BEHAVIOR USER AGREEMENT

I acknowledge receipt of, understand my responsibilities, and will comply with the Rules of Behavior for PRISM. I understand that failure to abide by the above rules and responsibilities may lead to disciplinary action up to and including dismissal. I further understand that violation of these rules and responsibilities may be prosecutable under District of Columbia and/or Federal law.

Signature

Date

APPENDIX A – SUSPICIOUS EXECUTABLE FILE TYPES

ADE - Microsoft Access Project Extension	ADP - Microsoft Access Project	BAS - Visual Basic Class Module	BAT - Batch File	CHM - Compiled HTML Help File
CMD - Windows NT Command Script	COM - MS-DOS Application	CPL - Control Panel Extension	CRT - Security Certificate	DLL - Dynamic Link Library
DOC or DOT - Word Documents and Templates	EXE - Application HLP - Windows Help File	INF - Setup Information File	INS - Internet Communication Settings	ISP - Internet Communication Settings
JS - JScript File	JSE - JScript Encoded Script File	LNK - Shortcut	MDB - Microsoft Access Application	MDE - Microsoft Access MDE Database
M SC - Microsoft Common Console Document	MSI - Windows Installer Package	MSP - Windows Installer Patch	MST - Visual Test Source File	OCX - ActiveX Objects
PCD - Photo CD Image	PIF - Shortcut to MS-DOS Program	POT - PowerPoint Templates	PPT - PowerPoint Files	REG - Registration Entries
SCR - Screen Saver	SCT - Windows Script Component	SHB - Document Shortcut File	SHS - Shell Scrap Object	SYS - System Config/Driver
URL - Internet Shortcut (Uniform Resource Locator)	VB - VBScript File`	VBE - VBScript Encoded Script File	VBS - VBScript Script File	WSC - Windows Script Component
WSF - Windows Script File	WSH - Windows Scripting Host Settings File	XL* - Excel Files and Templates	ZIP – Compressed File potentially containing other harmful executable file types	