ADMINISTRATIVE MEMORANDUM No. 120

SUBJECT: Information Security Policy

CONSIDERING:

That the security and integrity of the information systems of the General Secretariat are critical to the continued functioning of the General Secretariat;

That every individual who is granted access to said information systems shares in the responsibility for the integrity and security of the systems as a condition of their employment or association with the General Secretariat;

That the Information Security Policy of the Organization must clearly reflect the security challenges that emerging technologies and applications pose to the functioning of the General Secretariat; and

That the purpose of this Administrative Memorandum is to establish clear guidelines for the information security policy that applies to all users of information systems of the General Secretariat;

THE DECISION:

1. The Information Security Policy as set forth in the document attached as Appendix A is hereby adopted.

2. This Administrative Memorandum shall supersede any previous policies and practices of the General Secretariat on information security.

3. This Administrative Memorandum shall take effect on the date of its signature.

Gerald C. Anderson  
Secretary for Administration and Finance

Date: June 29, 2012
Original: English
# Information Security Policies

OAS-DOITS-PLC-Information Security

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.8</td>
<td>Approved</td>
</tr>
</tbody>
</table>

Table of Contents

1 SCOPE .................................................................................................................. 6

2 GENERAL CONSIDERATIONS .......................................................................... 6
  2.1 Use of Information Security Documentation............................................... 6
  2.2 Documented Ownership of Information Security Policies ....................... 6
  2.3 Communication of Information Security Policies ..................................... 6
  2.4 No Waiver ....................................................................................................... 6

3 INFORMATION SECURITY ROLES AND RESPONSIBILITIES .................... 7
  3.1 Centralized Information Security ................................................................. 7
  3.2 Ultimate Decision Maker on Information Security Matters .................... 7
  3.3 Information Systems Change Approval ...................................................... 7

4 INFORMATION AND ASSET MANAGEMENT .................................................. 8
  4.1 Use of Information and Damage Disclaimer............................................... 8
    4.1.1 Use of Information .................................................................................. 8
    4.1.2 Data and Program Damage Disclaimers .............................................. 8
  4.2 Information Ownership ................................................................................. 8
    4.2.1 File and Message Ownership ............................................................... 8
    4.2.2 Work Related Communications and Information ............................... 8
  4.3 Assets Procurement and Tracking .............................................................. 9
    4.3.1 Hardware and Software Procurement ............................................... 9
    4.3.2 Equipment Tracking ............................................................................ 9
  4.4 Loss ............................................................................................................... 9
    4.4.1 Off-Site Systems Damage and Loss .................................................... 9
    4.4.2 Reporting Loss or Unauthorized Activity .......................................... 9
  4.5 Software Copying .......................................................................................... 9
    4.5.1 Software Duplication ......................................................................... 9
    4.5.2 Unauthorized Copyrighted Material .................................................. 10

5 GS/OAS USERS ................................................................................................. 11
  5.1 Prior to Employment .................................................................................... 11
    5.1.1 Revealing Information to Prospective Employees ............................. 11
  5.2 During Employment ..................................................................................... 11
    5.2.1 GS/OAS Users Status Changes .......................................................... 11
    5.2.2 GS/OAS Users Computers ................................................................. 11
  5.3 Disciplinary Process ..................................................................................... 11
    5.3.1 Consequences of Non-Compliance .................................................... 11
  5.4 Termination or Change of Employment ...................................................... 11
    5.4.1 Return of Property at Termination ...................................................... 11
    5.4.2 Information Retention at Termination or Transfer ......................... 11
    5.4.3 Responsibility Transfer ...................................................................... 12
    5.4.4 Deletion of Terminated GS/OAS Users Files .................................... 12
  5.5 Removal of Access Rights ........................................................................... 12
    5.5.1 Physical Access of Terminated GS/OAS Users ................................. 12
    5.5.2 Computers of GS/OAS Users Terminated for Cause ..................... 12

6 EXTERNAL PARTIES ......................................................................................... 13
  6.1 Identification of Risks Related to Non-GS/OAS Users ............................ 13
6.1.1  THIRD-PARTY USERNAMES .......................................................... 13
6.1.2  LIMITED ACCESS TO NON-GS/OAS USERS ............................ 13
6.2  ADDRESSING SECURITY IN EXTERNAL PARTY AGREEMENTS .... 13
  6.2.1  INFORMATION SECURITY COMPLIANCE OF EXTERNAL PARTIES. 13
  6.2.2  INFORMATION TRANSFER TO EXTERNAL PARTIES ............... 13
  6.2.3  NETWORK-CONNECTED EXTERNAL PARTY SYSTEMS .......... 13
  6.2.4  INFORMATION RETURN BY EXTERNAL PARTIES .............. 13

7  PHYSICAL SECURITY ............................................................................. 14
  7.1  RESTRICTED AREAS ...................................................................... 14
   7.1.1  PHYSICAL ENTRY CONTROLS .................................................... 14
      7.1.1.1  Computer Center Staff Access ........................................ 14
      7.1.1.2  Unauthorized Physical Access Attempts .................. 14
      7.1.1.3  Visitor Identification .................................................... 14
      7.1.1.4  External Party Supervision ......................................... 14
      7.1.1.5  Data Center and DOITS Visitors .............................. 14
      7.1.1.6  Access to Computers and Communications Systems ... 14
      7.1.1.7  Securing Propped-Open Computer Center Doors ...... 14
   7.1.2  WORKING IN SAF/DOITS RESTRICTED AREAS .................. 15
      7.1.2.1  External Party Service Providers Working During Office Hours 15
      7.1.2.2  Communications Equipment Areas .......................... 15
      7.1.2.3  Repair People Who Show Up Without Being Called ...... 15
   7.2  EQUIPMENT SECURITY ................................................................ 15
      7.2.1  EQUIPMENT SITING AND PROTECTION ............................. 15
         7.2.1.1  Production Computer System Location ................. 15
         7.2.1.2  Computer Center Environmental Controls ........... 15
         7.2.1.3  Equipment Isolation .................................................. 15
      7.2.2  SECURITY OF EQUIPMENT OFF-PREMISES ....................... 15
         7.2.2.1  Computer Equipment Assignment and End of life ...... 16
         7.2.2.2  Mobile Devices must be returned for Decommission ... 16

8  OPERATIONS MANAGEMENT .............................................................. 17
  8.1  CHANGE MANAGEMENT ............................................................... 17
     8.1.1  PRODUCTION CHANGES ....................................................... 17
     8.1.2  PRODUCTION OPERATING SYSTEM CHANGES ................... 17
     8.1.3  SOFTWARE PATCHES, BUG FIXES AND UPGRADES ........ 17
     8.1.4  NEW TECHNOLOGY EVALUATION .................................... 17
  8.2  SEGREGATION OF DUTIES ............................................................ 17
     8.2.1  ENVIRONMENT SEPARATION ............................................ 17
     8.2.2  SOFTWARE TESTING ......................................................... 17
  8.3  CAPACITY MANAGEMENT ............................................................... 17
     8.3.1  USER PROCESSES, SESSIONS AND FILES ................... 17
     8.3.2  SYSTEM AVAILABILITY .................................................... 18
     8.3.3  MONITORING AND RECORDING USAGE ........................... 18
  8.4  SYSTEM ACCEPTANCE ................................................................. 18
     8.4.1  PRODUCTION SYSTEM ACCEPTANCE ............................... 18

9  BACK UP ............................................................................................ 19
  9.1  GS/OAS USERS BACKUP ........................................................... 19
  9.2  BACKUP OF DATA ON COMPUTER REPLACEMENT .................. 19
  9.3  BACKUP OF UNAUTHORIZED FILES ........................................ 19
  9.4  ON-SITE BACKUP FILES .......................................................... 19
  9.5  MULTIPLE BACKUP COPIES ....................................................... 19
9.6 Backup Information Review ................................................................. 19
9.7 Backup Media Fire Zone ..................................................................... 19
9.8 Backup Media Storage Units ............................................................. 19

10 Network Security Management ......................................................... 21
10.1 Security Configuration ..................................................................... 21
10.2 Disabling Critical Security Components .......................................... 21
10.3 Internal Network Addresses ............................................................ 21
10.4 Network Ports in Vacant Offices .................................................... 21
10.5 Implementing Multi-User Systems ................................................... 21
10.6 Computers Connected to Network Ports ........................................ 21
10.7 Internet Servers Firewalls ............................................................... 21
10.8 Internet Access ................................................................................. 22
10.9 Information in FTP Servers ............................................................. 22
10.10 Wireless Network Management ...................................................... 22
10.11 Remote Access Management ........................................................ 22
10.11.1 Remote Administration ............................................................... 22
10.11.2 Remote Access .......................................................................... 22

11 Exchange of Information .................................................................... 23
11.1 Information Disclosure ..................................................................... 23
  11.1.1 Information Disclosure: GS/OAS Passwords ................................ 23
  11.1.2 Sensitive Information on Answering Machines ............................. 23
  11.1.3 Distribution of Marketing Materials ........................................... 23
11.2 Copyright ......................................................................................... 23
  11.2.1 Copyright Protection ................................................................. 23
  11.2.2 Redistribution of Information Posted On-Line .............................. 23
11.3 E-mail ............................................................................................. 24
  11.3.1 Centralized Control Over Electronic Mail Systems ....................... 24
  11.3.2 Electronic Mail Message Monitoring ......................................... 24
  11.3.3 Signatures in Electronic Mail ..................................................... 24
  11.3.4 Electronic Mail Message Storage Schedule ............................... 24
  11.3.5 Sending Unsolicited Electronic Mail .......................................... 24
  11.3.6 Electronic Mail Broadcasts ....................................................... 24
  11.3.7 Message Content Restrictions .................................................. 24
  11.3.8 Responding to Spam Messages ................................................ 25
  11.3.9 Electronic Mail Attachments ..................................................... 25

12 Organizational Information Systems .................................................... 26
12.1 GS/OAS Standard Software ............................................................ 26
12.2 GS/OAS Computer Software Upgrades ......................................... 26
12.3 Computer Hardware Modifications ................................................ 26
12.4 Centralized Authorization for Use of New Information Services .......... 26
12.5 Accepting Security Assistance from Outside Parties ......................... 26
12.6 Eradicating Computer Viruses ........................................................ 26
12.7 Antivirus Software Installation ........................................................ 26
12.8 Involvement with Computer Viruses .............................................. 26
12.9 GS/OAS Official Portable Computer Backups .................................. 27
12.10 Device Synchronization ................................................................. 27
12.11 Computer System Names ............................................................... 27
12.12 Moving Office Computer Equipment .......................................... 27
12.13 Exploiting Systems Security Vulnerabilities ................................... 27
13  **INTERNET AND WEB SERVICES** ........................................... 28
   13.1  **PUBLICLY AVAILABLE INFORMATION** .................................. 28
   13.1.1  **IDENTITY MISREPRESENTATION** ..................................... 28
   13.1.2  **OUTBOUND INTERNET COMMUNICATIONS** .......................... 28
   13.1.3  **INTERNET NEWS SOURCES** ......................................... 28
   13.2  **GS/OAS WEBSITES** .................................................. 28
       13.2.1  **INTERNET DOMAIN NAME AND HOST NAME APPROVAL PROCESS** 28
       13.2.2  **INTERNET WEB PAGE MANAGEMENT COMMITTEE** .................. 28
       13.2.3  **INTERNET WEB PAGE DESIGN** .................................... 28
       13.2.4  **INTERNET DOMAIN NAME REGISTRATION** ........................... 28
       13.2.5  **INTRANET INFORMATION OWNER** .................................. 29
       13.2.6  **REMOVING OFFENSIVE MATERIAL** .................................. 29
14  **USER ACCESS MANAGEMENT** .............................................. 30
   14.1  **USER ACCOUNTS** .................................................... 30
       14.1.1  **UNIQUE USERNAME AND PASSWORD REQUIRED** ...................... 30
       14.1.2  **SYSTEM ACCESS REQUEST AUTHORIZATION** ......................... 30
       14.1.3  **PASSWORD EXPIRATION** ............................................ 30
       14.1.4  **PASSWORD LOCKOUTS** ............................................. 30
       14.1.5  **NETWORK LOGON BANNER** .......................................... 30
       14.1.6  **SPECIAL SYSTEM PRIVILEGES** ..................................... 30
       14.1.7  **SYSTEMS ADMINISTRATOR USERNAMES** ................................ 30
       14.1.8  **PERIODIC AUDIT REVIEW OF SYSTEM ACCESS CONTROL PRIVILEGES** 31
   14.2  **PASSWORD CREATION AND USE** ....................................... 31
       14.2.1  **PASSWORD STRUCTURE** ............................................. 31
       14.2.2  **TYPING PASSWORDS WHEN OTHERS ARE WATCHING** ................... 31
       14.2.3  **STORAGE OF PASSWORDS IN READABLE FORM** ........................ 31
       14.2.4  **PASSWORD CHANGE ON NEW ACCOUNT** ................................ 31
       14.2.5  **SUSPECTED PASSWORD DISCLOSURE** ................................ 31
       14.2.6  **PUBLIC PASSWORD DISCLOSURE** .................................... 31
       14.2.7  **PASSWORD SHARING** ............................................. 32
       14.2.8  **EXTERNAL PARTY PASSWORD USAGE** ................................ 32
       14.2.9  **RESPONSIBILITY ABOUT PERSONAL USERNAMES** .................... 32
       14.2.10  **DISCLOSURE OF SENSITIVE INFORMATION** ........................... 32
       14.2.11  **UNATTENDED ACTIVE SESSIONS** ................................... 32
15  **INFORMATION SYSTEMS DEVELOPMENT AND MAINTENANCE** ....... 33
   15.1  **OPERATING SYSTEM USER AUTHENTICATION** .......................... 33
   15.2  **USE OF SOFTWARE TOOLS AND LANGUAGES** ........................ 33
   15.3  **SECRET USERNAMES OR PASSWORDS** .................................. 33
   15.4  **CREATING SECURITY TOOLS** .......................................... 33
   15.5  **PRODUCTION SYSTEM CONTROLS** ..................................... 33
   15.6  **SOFTWARE ENVIRONMENT TRANSFER** .................................. 33
   15.7  **ACCESS PATHS IN PRODUCTION SOFTWARE** ............................. 33
   15.8  **PROPERTY RIGHTS** ................................................... 34
   15.9  **THIRD PARTY SOFTWARE DEVELOPERS ACCESS TO SOURCE CODE** ....... 34
   15.10  **APPLICATION CODING PRINCIPLES** ................................... 34
   15.11  **MATURE DEVELOPMENT TOOLS AND TECHNIQUES** ..................... 34
   15.12  **TRACING ERRORS AND SECURITY PROBLEMS TO DEVELOPERS** .......... 34
16  **ANNEX 1 - GLOSSARY** ................................................... 35
17  **ANNEX 2 – REFERENCED DOCUMENTS** .................................... 38
1 Scope

These Policies cover usage of the General Secretariat (GS) of the Organization of American States (OAS) information technology infrastructure and user computer equipment and services.

All GS/OAS users must read, understand and comply with the policies outlined in this and in its referenced documents.

By signing onto the network, all GS/OAS users shall acknowledge that they are obligated to abide by the Information Security Policies of the GS/OAS, including this Administrative Memorandum and shall be required to click their acceptance of these Policies.

2 General Considerations

2.1 Use of Information Security Documentation

All GS/OAS information security documentation including, but not limited to, policies, standards, and procedures, is considered proprietary information of the GS/OAS and its unauthorized disclosure to third parties outside the GS/OAS is prohibited.

2.2 Documented Ownership of Information Security Policies

All GS/OAS information security policies, standards and procedures must have a custodian. The custodian is the Information Security Section in the Department of Information and Technology Services (DOITS).

2.3 Communication of Information Security Policies

The Secretariat for Administration and Finance (SAF) is responsible for communicating the Information Security Policies of the GS/OAS and make them available to GS/OAS users and relevant external parties.

2.4 No Waiver

Any failure of GS/OAS to enforce any requirement with regard to the Information Security Policies does not constitute a waiver of said Policies, and does not constitute its consent to the continued breach of Information Security Policies. Regardless of prior history of enforcement, GS/OAS users and relevant external parties are bound by and shall comply with the Information Security Policies of GS/OAS.
3 Information Security Roles and Responsibilities

3.1 Centralized Information Security

Management of all information security activities is centralized for the entire Organization in the SAF/DOITS, through the Information Security Section.

3.2 Ultimate Decision Maker on Information Security Matters

SAF/DOITS Director is the ultimate decision maker on all matters relating to information security at GS/OAS.

3.3 Information Systems Change Approval

Department managers or other members of the management team must not initiate any procurement, sign contracts, initiate internal projects, or otherwise make promises that obligate GS/OAS to make changes in the Organization’s IT environment, unless these changes are pre-approved by SAF/DOITS Director.
4  Information and Asset Management

4.1  Use of Information and Damage Disclaimer

4.1.1  Use of Information

GS/OAS information must be used only for those organizational purposes expressly authorized by management. All non-approved usage of GS/OAS information is explicitly prohibited.

4.1.2  Data and Program Damage Disclaimers

GS/OAS uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by its computers and communications systems. In keeping with these objectives, GS/OAS maintains the authority to:

Restrict or revoke any GS/OAS users and relevant external parties’ privileges to use GS/OAS computers and communications systems.

Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine the objectives of confidentiality, integrity and availability of the information handled by GS/OAS computers and communications systems.

GS/OAS reserves the right to take any other steps it deems necessary to protect its information systems. This authority shall be exercised with notice to the involved GS/OAS users or relevant external parties, except in circumstances where access is provided pursuant to a confidential investigation conducted pursuant to GS/OAS norms and procedures or other extenuating circumstances.

4.2  Information Ownership

4.2.1  File and Message Ownership

GS/OAS has legal ownership of the contents of all files and messages stored or transmitted on its computers and communications systems, and reserves the right to access this information without prior notice whenever there is a genuine organizational need. Any SAF/DOITS intervention will be documented and communicated in writing to the Secretary of the involved area unless the intervention involves confidential information or communications that of which the relevant Secretary is not authorized to have knowledge. Additionally, SAF/DOITS will give prior written notice of said intervention to the Office of Inspector General.

4.2.2  Work Related Communications and Information

Subject to the stated exceptions, it shall be a violation of these Policies for any GS/OAS user or network administrator or any relevant external party to knowingly intercept, alter, or disseminate any work-related communication or work-related information not intended for or addressed to the recipient(s) listed in the communication or information. Subject to stated exceptions, it shall also be a violation of these Policies for any party to intercept, read, or disseminate information or work-product produced contained or stored in any GS/OAS user’s computer or memory device without the consent of the GS/OAS user who produced the work-related information or product.
Stated Exceptions as referenced above include inquiries or investigations of the GS/OAS Office of Inspector General or Board of External Auditors; specific written inquiries made by a disciplinary body as a result of a disciplinary proceeding instituted per the General Standards and Staff Rules; specific written inquiries from the Department of Legal Services directly related to litigation or preparation for litigation; specific written inquiries from the governing organs of the OAS; and matters the Secretary General deems necessary to avoid the impediment of the course of justice in any Member State. In response to any inquiry that falls under a stated exception above, the General Secretariat reserves the right at its sole discretion to adjust responses to requests that are overly broad, or lack specificity, or address matters that are not work-related. The Department of Legal Services may be consulted with regard to the applicability of any stated exception. Communications or data that are not work-related are not protected from the above-referenced prohibition against interception or dissemination, and shall be handled at the discretion of those GS/OAS staff charged with the responsibility for information technology and communication.

4.3 Assets Procurement and Tracking

4.3.1 Hardware and Software Procurement

All GS/OAS hardware and software must be procured through the Office of Procurement Services, according to GS/OAS IT compatibility standards, Administrative Memorandums 117,118, and must be authorized by SAF/DOITS.

4.3.2 Equipment Tracking

All GS/OAS hardware and communications equipment must have a unique computer-readable identifier attached to it such that physical inventories can be efficiently conducted. The SAF shall be the custodian of the list of computer-readable identifiers, and shall regularly update the list as necessary. SAF shall also be responsible for performing physical inventories of equipment.

4.4 Loss

4.4.1 Off-Site Systems Damage and Loss

GS/OAS users and relevant external parties must promptly report to their manager any damage to or loss of GS/OAS computer hardware, software, or information that has been entrusted to their care.

4.4.2 Reporting Loss or Unauthorized Activity

GS/OAS users and relevant external parties must immediately report to SAF/DOITS Information Security Section any loss of, or unauthorized changes to, computerized data.

4.5 Software Copying

4.5.1 Software Duplication

GS/OAS users and relevant external parties must not copy software provided by GS/OAS to any storage media, transfer such software to another computer, or disclose such software to outside parties.
4.5.2 Unauthorized Copyrighted Material

GS/OAS users and relevant external parties are strictly prohibited from participating in any manner with pirated software bulletin boards or related Internet sites. This prohibition extends to any other facility or system that exchanges illegal copies of music, books, or other copyrighted material over the Internet or through other communications channels.
5 GS/OAS users

5.1 Prior to Employment

5.1.1 Revealing Information to Prospective Employees

Information systems technical details, such as network addresses and network diagrams among others, must not be revealed to GS/OAS job applicants until they have been hired or retained.

5.2 During Employment

5.2.1 GS/OAS users Status Changes

Every change in the organizational status of GS/OAS users must be immediately reported by the Department of Human Resources to SAF/DOITS.

5.2.2 GS/OAS users Computers

GS/OAS users shall be assigned no more than one desktop computer.

5.3 Disciplinary Process

5.3.1 Consequences of Non-Compliance

Non-compliance with information security policies, standards, or procedures can subject GS/OAS users to disciplinary measures according to the Staff Rules, including Summary Dismissal, or termination for cause of CPR contracts or other contracts.

5.4 Termination or Change of Employment

5.4.1 Return of Property at Termination

At the time that every GS/OAS employee terminates his or her relationship with GS/OAS, every GS/OAS employee must fill form FA-323 to validate the return of all GS/OAS property.

5.4.2 Information Retention at Termination or Transfer

Upon termination of employment or transfer to another GS/OAS department or area, GS/OAS users may not retain, give away or remove from GS/OAS premises any GS/OAS information, unless appropriate written authorization has been sent to SAF/DOITS. In the case that the GS/OAS user needs to access this information, a written authorization from the Director of the incumbent department (or Secretary for the incumbent Secretariat as the case may be) must be sent to SAF/DOITS.
5.4.3 Responsibility Transfer

Before a GS/OAS user leaves any position in the Organization, his or her immediate manager, with the assistance of SAF/DOITS helpdesk, must review all of his or her computer resident files, reassign his or her duties, and specifically delegate responsibility for the files formerly in his or her possession. After the GS/OAS user leaves his or her position, GS/OAS will not be responsible for any lost information.

5.4.4 Deletion of Terminated GS/OAS users Files

Unless SAF/DOITS has received instructions to the contrary, after a GS/OAS user has permanently left GS/OAS, all files held in the correspondent computer must be purged.

5.5 Removal of Access Rights

5.5.1 Physical Access of Terminated GS/OAS users

When a GS/OAS user terminates his or her working relationship with GS/OAS, all physical security access codes known by, or available to, said GS/OAS user to access SAF/DOITS restricted areas, must be deactivated or changed by the Office of General Services (OGS)

5.5.2 Computers of GS/OAS Users Terminated for cause.

All GS/OAS users summarily dismissed, terminated for cause, or under administrative leave must have their computers immediately isolated from both the Internet and the internal GS/OAS network. Before being used for any other GS/OAS purpose, these computers must have their hard drives backed-up and then reformatted, at which point the appropriate systems software must be reinstalled.
6 External Parties

6.1 Identification of risks related to non-GS/OAS users

6.1.1 Third-Party Usernames

Individuals, who are not GS/OAS users or relevant external parties, must not be granted a network account or be given privileges to use GS/OAS computers or communications systems unless the written approval of a department head has first been obtained by SAF/DOITS, and approved by the Department of Human Resources.

6.1.2 Limited Access to Non-GS/OAS Users

Activities requiring access to sensitive GS/OAS information must only be performed by GS/OAS users unless the requisite knowledge or skills are not possessed by GS/OAS users or an emergency or disaster requires the use of external parties, or permission of the SAF/DOITS has been obtained.

6.2 Addressing Security in External Party Agreements

6.2.1 Information Security Compliance of External Parties

External parties, in order to be granted access to the GS/OAS computer network must be subject to the same information security requirements, and have the same information security responsibilities as GS/OAS users.

6.2.2 Information Transfer to External Parties

GS/OAS software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-GS/OAS external party for any purposes other than those expressly authorized by GS/OAS, in coordination with SAF/DOITS.

6.2.3 Network-Connected External Party Systems

As a condition of gaining access to GS/OAS’ computer network, every relevant external party must secure its own connected systems in a manner consistent with GS/OAS requirements. GS/OAS reserves the right to audit the security measures in effect on these connected systems without prior warning. GS/OAS also reserves the right to immediately terminate network connections with all external party systems. Such a disconnection would be warranted if GS/OAS believes the external party is not meeting these requirements, or if the external party is providing an avenue of attack against GS/OAS systems.

6.2.4 Information Return by External Parties

Upon the termination or expiration of their contract, all relevant external parties, must give their project manager all copies of GS/OAS information received or created during the execution of the contract.
7 Physical Security

7.1 Restricted Areas

7.1.1 Physical Entry Controls

7.1.1.1 Computer Center Staff Access

The Information Security Section of SAF/DOITS shall maintain on a quarterly basis, and update when necessary, a list of all GS/OAS users who are authorized to access the datacenter.

7.1.1.2 Unauthorized Physical Access Attempts

GS/OAS users must not attempt to enter restricted areas in GS/OAS buildings for which they have not received access authorization.

7.1.1.3 Visitor Identification

All visitors to GS/OAS must sign a log prior to gaining access to restricted areas.

7.1.1.4 External Party Supervision

Individuals, who are not SAF/DOITS personnel, nor specifically authorized external parties, must be supervised whenever they are in restricted SAF/DOITS areas.

7.1.1.5 Data Center and DOITS Visitors

Visitors who do not need to perform maintenance on GS/OAS equipment, or who do not absolutely need to be inside the Data Center or the Department of Information and Technology Services, must not enter these areas.

7.1.1.6 Access to Computers and Communications Systems

Buildings that house GS/OAS computers or communications systems must be protected with physical security measures that prevent unauthorized persons from gaining access.

7.1.1.7 Securing Propped-Open Computer Center Doors

Whenever doors to the computer center are propped-open, a SAF/DOITS employee or a security guard from the Physical Security Department must continuously monitor the entrance.
7.1.2 Working in SAF/DOITS restricted areas

7.1.2.1 External Party Service Providers Working During Office Hours

All external party service providers (including maintenance, repair, construction, and information systems) must do their in-person work on GS/OAS premises during regular GS/OAS business hours. Exceptions will be made only if SAF/DOITS approval is obtained in advance, and if these service providers are continuously escorted while on GS/OAS premises.

7.1.2.2 Communications Equipment Areas

Telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing communications equipment must be kept locked at all times and not accessed by visitors or GS/OAS users without an authorized technical staff escort to monitor all work being performed.

7.1.2.3 Repair People Who Show Up Without Being Called

Every external party repair person or maintenance person who shows up at GS/OAS facilities without being called by SAF/DOITS personnel must be denied access to the facilities. All such incidents must be promptly reported to GS/OAS Security Guards. Those that have been called by SAF/DOITS personnel must have their requested presence confirmed by a guard or receptionist before they are given access to the facilities.

7.2 Equipment Security

7.2.1 Equipment Sitting and Protection

7.2.1.1 Production Computer System Location

All multi-user production computer systems including, but not limited to, servers, firewalls, routers, must be physically located within a secure data center.

7.2.1.2 Computer Center Environmental Controls

The Office of General Services must provide and adequately maintain fire detection and suppression, power conditioning, air conditioning, humidity control, and other computing environment protection systems in every GS/OAS computer data center.

7.2.1.3 Equipment Isolation

Computer and communications equipment managed by GS/OAS users must be physically isolated from equipment managed by third parties.

7.2.2 Security of Equipment off-premises
7.2.2.1 Computer Equipment Assignment and End of life

SAF/DOITS is responsible for uninstalling computers and printers no longer needed for organizational activities. SAF/DOITS is the only body responsible and the only decision maker for the assignment of computers to GS/OAS users and relevant external parties.

7.2.2.2 Mobile Devices must be returned for Decommission

All GS/OAS issued smart phones and cell phones must be returned to SAF/DOITS, when no longer in use by GS/OAS users or relevant external parties.
8 Operations Management

8.1 Change Management

8.1.1 Production Changes

Changes to GS/OAS production computer programs must only be performed by SAF/DOITS Infrastructure Section personnel. In the case of Database structural changes, they must only be performed by SAF/DOITS Information Structuring Section.

8.1.2 Production Operating System Changes

Extensions, modifications, or replacements to production operating system software must be made only if the written approval of the SAF/DOITS Director has been received in advance.

8.1.3 Software Patches, Bug Fixes and Upgrades

All GS/OAS networked production systems must follow a process to review and install all new released systems software patches, bug fixes, and upgrades.

8.1.4 New Technology Evaluation

Before any new technology is used with GS/OAS production application software or hardware systems or network, the new technology must be evaluated and approved by SAF/DOITS.

8.2 Segregation of Duties

8.2.1 Environment Separation

GS/OAS application software in development must be kept strictly separate from production application software through physically separate computer systems, or separate directories or libraries with strictly enforced access controls.

8.2.2 Software Testing

GS/OAS users who have been involved in the development of specific GS/OAS application software must not be involved in the formal testing or day-to-day production operation of such software.

8.3 Capacity management

8.3.1 User Processes, Sessions and Files

GS/OAS may alter the priority of, or terminate the execution of, any user process that it believes is consuming excessive system resources or is significantly degrading system response time, terminate user sessions or connections if this usage is deemed to be in violation of security policies or consuming excessive system resources, or remove or compress user disk files if it believes these files consume excessive disk space. GS/OAS shall notify the GS/OAS user before undertaking such action, if reasonably possible, and if not, immediately thereafter.
8.3.2 System Availability

GS/OAS users must be able to access all shared computer systems according to SAF/DOITS SLAs.

8.3.3 Monitoring and Recording Usage

The usage of all GS/OAS shared computing resources employed for production activities must be continuously monitored and recorded. This usage history data must in turn be provided in real-time to those security alert systems designated by the Information Security Section.

8.4 System Acceptance

8.4.1 Production System Acceptance

Before being used for production processing, new or substantially changed GS/OAS application systems must have received written approval from the SAF/DOITS Software Quality Assurance Section and Information Security Section, according to the OAS-SDF.
9 Back Up

9.1 GS/OAS Users Backup

SAF/DOITS does not make backups of GS/OAS users’ personal or working data and will provide backup of organizational data as needed.

9.2 Backup of data on computer replacement

When a GS/OAS user is assigned a new computer, it is his or her responsibility to specify in writing the location of the working files in his or her computer and give a clear indication of their importance for his or her work. It is the GS/OAS user’s responsibility to verify his or her files are fully transferred to the new computer.

9.3 Backup of unauthorized files

SAF/DOITS Helpdesk must not transfer personal data files when a GS/OAS user’s workstation is replaced.

9.4 On-Site Backup Files

At least one generation of backup files must be maintained on off-line data storage media by SAF/DOITS, wherever production servers are located, according to GS/OAS Backup Standard.

9.5 Multiple Backup Copies

At least two recent and complete backups made on different dates containing critical GS/OAS records must always be stored off-site.

9.6 Backup Information Review

All files and messages stored on GS/OAS critical servers are routinely copied to tape and disk. These backups must be recoverable for potential examination at a later date by Systems Administrators and others designated by SAF/DOITS Director.

9.7 Backup Media Fire Zone

Computer and network backup storage media must be stored in a separate fire zone from the machine producing the backup.

9.8 Backup Media Storage Units

Unless they have a closing mechanism that is triggered by a fire alarm, all areas where backup media is stored including, but not limited to, fireproof computer backup storage rooms, vaults, and cabinets must be kept fully closed when not in active use.
10  Network Security Management

10.1 Security Configuration

Configurations and set-up parameters on all hosts attached to the GS/OAS network must comply with GS/OAS security policies and standards.

10.2 Disabling Critical Security Components

Critical components of GS/OAS information security infrastructure must not be disabled, bypassed, turned off, or disconnected unless otherwise stated by SAF/DOITS.

10.3 Internal Network Addresses

The internal system addresses, configurations, and related system design information for GS/OAS networked computer systems must be restricted such that both systems and users outside the GS/OAS internal network cannot access this information.

10.4 Network Ports in Vacant Offices

All network ports in vacant offices and other areas that are not customarily in use must be promptly disconnected at the wiring closet or at another centralized location.

10.5 Implementing Multi-User Systems

GS/OAS users and relevant external parties must not establish intranet servers, local area networks, modem connections to existing internal networks, wireless network access points, or connect smartphones, PDAs or other multi-user systems.

10.6 Computers connected to network ports

GS/OAS computer equipment must be directly connected to GS/OAS network ports. No hubs, switches or wireless routers must be used to connect more than one computer to a GS/OAS network port.

10.7 Internet Servers Firewalls

All GS/OAS servers directly connected to the Internet must be protected by GS/OAS firewalls managed by SAF/DOITS.
10.8 Internet Access

All Internet access using computers in GS/OAS offices must be routed through GS/OAS internet connection and GS/OAS firewall.

10.9 Information in FTP Servers

All publicly modifiable directories on GS/OAS FTP servers must be reviewed and cleared every six months.

10.10 Wireless Network Management

All wireless access points must be installed by, configured by, and administered by SAF/DOITS.

10.11 Remote Access Management

10.11.1 Remote Administration

Remote administration of Internet-connected computers must be performed only over encrypted links and only by SAF/DOITS authorized personnel.

10.11.2 Remote Access

Remote access accounts and passwords of GS/OAS users and relevant external parties are non-transferable and must not be shared. GS/OAS users and relevant external parties must not login and use their remote access credentials on more than one computer device at the same time.
11 Exchange of Information

11.1 Information Disclosure

11.1.1 Information Disclosure: GS/OAS passwords

No GS/OAS user or relevant external party may disclose his or her GS/OAS passwords.

11.1.2 Sensitive Information on Answering Machines

GS/OAS users and relevant external parties must not record messages containing sensitive information on answering machines or voice mail systems.

11.1.3 Distribution of Marketing Materials

GS/OAS users and relevant external parties must not use facsimile machines, electronic mail, auto-dialer robot voice systems, or any other electronic communications systems for the distribution of unsolicited advertising material.

11.2 Copyright

11.2.1 Copyright Protection

Most of the material on the Internet is copyrighted or otherwise protected by intellectual property law. GS/OAS users and relevant external parties must investigate intellectual property rights for all material they discover on the Internet before using it for any other purpose. For example, GS/OAS cannot use photographs found in newspapers or magazines in OAS circulars or publications without the consent of the party who owns the intellectual property rights in those photographs.

11.2.2 Redistribution of Information Posted On-Line

GS/OAS users and relevant external parties using GS/OAS computers and communication systems must not redistribute information (music, software, graphics, text, among others) that they access via the Internet unless they have confirmed that such redistribution is expressly permitted by the copyright owner. All information accessed, must be assumed to be copyrighted unless a notice to the contrary is found.

All GS/OAS users and relevant external parties, who redistribute such information shall accept sole responsibility and hold the GS/OAS harmless for any claims or damages brought by injured parties for the redistribution.
11.3 E-mail

11.3.1 Centralized Control over Electronic Mail Systems

Centralized control over both inbound and outbound electronic mail will be provided by SAF/DOITS. All GS/OAS electronic mail must flow through systems established, operated, and maintained by that same department.

11.3.2 Electronic Mail Message Monitoring

All GS/OAS electronic mail systems are to be used only for organizational purposes. All messages sent by electronic mail are GS/OAS property. GS/OAS reserves the right to access and disclose the content of all messages upon prior authorization of the Secretary General, or his or her designee, to the extent to which access and disclosure are provided for in GS/OAS norms and regulations.

11.3.3 Signatures in Electronic Mail

GS/OAS users must only use the electronic mail signature according to the norms established in executive order 09-1.

11.3.4 Electronic Mail Message Storage Schedule

GS/OAS users email mailboxes will be backed up for only six months. GS/OAS users are encouraged to delete messages they don't need and must regularly move important information from electronic mail message files to word processing documents, Outlook PSTs, and other files. Outlook PST must not be stored in shared network drives.

11.3.5 Sending Unsolicited Electronic Mail

GS/OAS users and relevant external parties must not send uninvited or unsolicited electronic mail (also known as spam) to a large number of recipients. This includes commercial advertisements, charitable solicitations, questionnaires/surveys, chain letters, and political statements. If a GS/OAS user or relevant external party does send spam and the recipients contact the GS/OAS mail system administrator with complaints, he or she will be subject to disciplinary action including loss of system privileges.

11.3.6 Electronic Mail Broadcasts

Broadcast facilities found in electronic mail systems must be used only by SAF/DOITS or only through SAF/DOITS alternative approved systems. Additionally, access to non-approved systems will be blocked.

11.3.7 Message Content Restrictions

GS/OAS users and relevant external parties must not send or forward any messages through GS/OAS information systems that may be considered defamatory, harassing, or explicitly sexual, or that would be likely to offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.
11.3.8 Responding To Spam Messages

To keep spam to a minimum, GS/OAS users must refrain from responding in any way to spam, must not purchase anything advertised in spam, must not post their email address in any public location (web sites, news groups, etc.), and must refrain from disclosing their email address unless it is absolutely needed to conduct GS/OAS organizational functions. When publishing an email address in any public statement, including newspaper advertisements and web pages, GS/OAS users must also seriously consider the use of a temporary email address.

11.3.9 Electronic Mail Attachments

GS/OAS users and relevant external parties must not open electronic mail attachments unless they were expected from a known and trusted sender, and unless these attachments have been scanned by GS/OAS antivirus software package.
12 Organizational Information Systems

12.1 GS/OAS Standard software

Only GS/OAS standard software must be installed on GS/OAS computers, according to “GS/OAS standard software for GS/OAS workstations” document.

12.2 GS/OAS Computer Software Upgrades

GS/OAS and relevant external parties are not allowed to install or upgrade programs on GS/OAS computer equipment. Installation of software must be performed by SAF/DOITS.

12.3 Computer Hardware Modifications

GS/OAS computer equipment must not be altered or added to in any way without SAF/DOITS authorization.

12.4 Centralized Authorization for Use of New Information Services

New information services, such as Internet-based collaboration tools, cloud computing services, instant messaging, non-standard GS/OAS software, must not be used or installed, unless these services have first been reviewed and approved by SAF/DOITS.

12.5 Accepting Security Assistance from Outside Parties

GS/OAS users must not accept any form of assistance to improve the security of GS/OAS computer equipment, without first having the provider of this assistance approved by SAF/DOITS. This means that GS/OAS users must not accept offers of consulting services, must not download security software via the Internet, and must not employ security posture evaluation web pages.

12.6 Eradicating Computer Viruses

GS/OAS users who suspect infection by a virus must immediately shut-down the involved computer and call the GS/OAS help desk, and make no attempt to eradicate the virus.

12.7 Antivirus Software Installation

Antivirus software must be installed and enabled on all GS/OAS Servers and GS/OAS computer equipment. This is a priority for SAF/DOITS.

12.8 Involvement with Computer Viruses
GS/OAS users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any GS/OAS computer equipment or network.

12.9 GS/OAS Official Portable Computer Backups

GS/OAS users who use official GS/OAS laptops must make backups of all critical information resident on these computers prior to taking out-of-town trips. These backups must be stored somewhere other than the portable computer’s carrying case.

12.10 Device Synchronization

Systems that automatically exchange data between devices, such as a personal digital assistant, smart phones and personal computers, must not be enabled unless the systems are part of the document “GS/OAS standard equipment”.

12.11 Computer System Names

The function performed by a computer or the software that it runs must not be used in any part of the computer’s name, if that name is visible from the GS/OAS internal network or occurs in any computer-readable file. GS/OAS computer equipment must comply with the document “GS/OAS computer names standard”.

12.12 Moving Office Computer Equipment

GS/OAS computer equipment must not be moved, relocated, stored or reassigned to other GS/OAS users, as provided on Administrative Memorandum No 117 – “Computer Equipment Acquisition Policy”.

12.13 Exploiting Systems Security Vulnerabilities

GS/OAS users and relevant external parties must not exploit vulnerabilities or deficiencies in information systems security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted.
13 Internet and Web Services

13.1 Publicly available information

13.1.1 Identity Misrepresentation

GS/OAS users must not misrepresent, obscure, suppress, or replace their own or another person's identity on any GS/OAS electronic communications.

13.1.2 Outbound Internet Communications

All outbound Internet communications must reflect the parameters established by the Secretariat of External Relations, for official communications of GS/OAS.

13.1.3 Internet News Sources

News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to GS/OAS organizational functions and the duties of the receiving GS/OAS users.

13.2 GS/OAS Websites

13.2.1 Internet Domain Name and Host Name Approval Process

Every Internet host server name, and every Internet web site name, which is run by or owned by GS/OAS, must be approved in advance of its use by the Secretariat of External Relations and SAF/DOITS.

13.2.2 Internet Web Page Management Committee

Prior to being posted, all changes to the GS/OAS Internet web site must be approved by a special committee (according to Executive Order 09-2) established by the Secretariat of External Relations that will ensure that all posted material has a consistent and polished appearance, is aligned with organizational goals, and is protected by adequate security measures.

13.2.3 Internet Web Page Design

All GS/OAS Internet web pages must conform to layout standards, navigation standards, and similar requirements specified by Executive Order 09-2.

13.2.4 Internet Domain Name Registration

Payments and paperwork for Internet domain name registrations for all of GS/OAS official sites must be handled in a timely manner and promptly confirmed by SER/Department of Press and Communications.
13.2.5 Intranet Information Owner

All information posted to the GS/OAS intranet must have a designated owner and the contact information for this owner must be clearly indicated on the page where the information appears.

13.2.6 Removing Offensive Material

GS/OAS retains the right to remove from its internal information systems any material that it views as offensive, abusive, or potentially illegal.
14 User Access Management

14.1 User Accounts

14.1.1 Unique Username and Password Required

GS/OAS users and relevant external parties must have a single unique Username and a personal secret password for access to GS/OAS computers and network resources. User ID and passwords must follow the standard documented in “User ID and Password Standard”.

14.1.2 System Access Request Authorization

All requests for additional privileges on GS/OAS multi-user systems or networks must be submitted to SAF/DOITS Information Security Section and authorized by the user’s immediate manager.

14.1.3 Password Expiration

Passwords for GS/OAS network accounts must be changed every six months from the time they are established and renewable in six-month intervals.

14.1.4 Password Lockouts

After five unsuccessful attempts to enter a password, the GS/OAS network account will be automatically locked out, until it has been reset by GS/OAS Helpdesk.

14.1.5 Network Logon Banner

A standard notice must be displayed when GS/OAS users and relevant external parties login to GS/OAS internal computer networks. This notice shall remind all users that they are bound to adhere to this Policy when accessing the network.

14.1.6 Special System Privileges

Special system privileges, such as the ability to examine the files of other GS/OAS users, must be restricted to those directly responsible for system management and/or systems security inside SAF/DOITS.

This authority shall be exercised with notice to the involved GS/OAS users or relevant external parties, except in circumstances where access is provided pursuant to a confidential investigation conducted pursuant to GS/OAS norms and procedures or other extenuating circumstances.

14.1.7 Systems Administrator Usernames

System administrators managing computer systems must have at least two Usernames, one that provides privileged access to servers, and the other that provides the privileges of a normal user for
day-to-day work. System administrators must never use privileged access Usernames to perform normal user day-to-day work.

14.1.8 Periodic Audit Review of System Access Control Privileges

SAF/DOITS Information Security Section must, on a quarterly basis, review the granted access privileges of network accounts with System Administration permissions. This review must reflect whether the GS/OAS users and relevant external parties have only those privileges necessary to perform their jobs and no additional privileges.

14.2 Password Creation and Use

14.2.1 Password Structure

GS/OAS users and relevant external parties must not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of Usernames, common character sequences or personal details.

14.2.2 Typing Passwords when Others are Watching

GS/OAS users and relevant external parties must never type their passwords at a keyboard or a telephone keypad if others are known to be observing the password being typed. To do so unduly exposes the information accessed thereby to unauthorized access.

14.2.3 Storage of Passwords in Readable Form

GS/OAS users and relevant external parties’ passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without enforced access control mechanisms, or in other locations where unauthorized persons might discover or use them.

14.2.4 Password Change on New Account

GS/OAS users and relevant external parties must immediately change their temporary password provided by helpdesk, the first time they use the account in order to sign-in to the GS/OAS network.

14.2.5 Suspected Password Disclosure

GS/OAS users and relevant external parties must immediately change their password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized person.

14.2.6 Public Password Disclosure

Passwords must not be written down and left in a place where unauthorized persons might discover them.
14.2.7 Password Sharing

Passwords must never be shared or revealed to anyone except when SAF/DOITS helpdesk creates a password for a new account, or resets a password.

14.2.8 External Party Password Usage

GS/OAS users and relevant external parties must not provide their Usernames and/or passwords to any outside parties. Such disclosures not only cause the involved GS/OAS users or relevant external parties to be responsible for all damage that party may cause, but this behavior is also a justifiable cause for GS/OAS to terminate the GS/OAS user or relevant external party's privileges on its systems.

14.2.9 Responsibility about Personal Usernames

GS/OAS users and relevant external parties must be responsible for all activity performed with their personal GS/OAS network accounts. They must not permit others to perform any activity with their network accounts, and they must not perform any activity with IDs belonging to other GS/OAS users.

14.2.10 Disclosure of Sensitive Information

GS/OAS will never ask you to reveal your password, your social security number, your account balance, or other sensitive information via regular email.

14.2.11 Unattended Active Sessions

GS/OAS users and relevant external parties must not leave their personal computer, workstation, or terminal unattended without logging out or locking the workstation.
15 Information Systems Development and Maintenance

15.1 Operating System User Authentication

Internal GS/OAS and third party developers must consistently rely on the access controls provided by the operating systems. Developers must not construct other mechanisms to collect or manage access control information, and they must not construct or install other mechanisms to identify or authenticate the identity of GS/OAS users or relevant external parties.

15.2 Use of Software Tools and Languages

Internal GS/OAS and third party developers must not use software tools and languages that have unproven security attributes when they build web sites, extranets, or any other system having an interface to external parties.

15.3 Secret Usernames or Passwords

Internal GS/OAS and third party developers must not build or deploy secret Usernames or passwords that have special privileges, and that are not clearly described in the generally available system documentation.

15.4 Creating Security Tools

Internal GS/OAS and third party developers must not create new security protocols, compose new security schemes, develop new encryption algorithms, or otherwise be inventive when it comes to information security.

15.5 Production System Controls

Before being used for production processing, new or substantially changed organizational application systems must have received written approval from SAF/DOITS Information Security Section.

15.6 Software Environment Transfer

Internal GS/OAS and third party developers must not have the ability to move any software into the production environment, according to “Verification and Validation Standard”.

15.7 Access Paths in Production Software

Internal GS/OAS and third party developers must remove all special access paths and system privileges prior to moving software to production environment.
15.8 Property Rights

Without specific written exceptions, all programs and documentation generated by, or provided by any GS/OAS users and relevant external parties for the benefit of GS/OAS are the property of GS/OAS. Management must ensure that all workers providing such programs or documentation sign a statement to this effect prior to the delivery of these materials to GS/OAS. Refer to CPR rules and Staff rules.

15.9 Third Party Software Developers Access to Source Code

Third party developers must not be granted direct access to GS/OAS source code. Only the modules needed for a specific programming task may be revealed to these programmers. These programmers must additionally never be given privileges to directly update GS/OAS production source or object code.

15.10 Application Coding Principles

Secure coding principles and practices must be used for all software developed or maintained in-house or by third parties according to the document “Application Security Standard”.

15.11 Mature Development Tools and Techniques

All software development projects must use GS/OAS standard development tools and techniques, according to OAS-SDF.

15.12 Tracing Errors and Security Problems to Developers

All complaints about software errors, omissions, and security problems that are attributable to software developed must be traced back to the Project Leader assigned by SAF/DOITS, according to OAS-SDF.
16 Annex 1 - Glossary

A

• **Access control**: A system to restrict the activities of users and processes based on “The concept of least privilege [which] refers to granting users only those accesses required to perform their duties”
• **Account**: See Username.

C

• **Confidential information**: Sensitive information whose disclosure is expected to damage the GS/GS/OAS and/or the GS/OAS. See Sensitive Information.
• **Critical information**: Any information essential to GS/OAS organizational activities, the destruction, modification, or unavailability of which would cause serious disruption to GS/OAS.

D

• **Default password**: A preselected password issued every time a new user ID is created, or the initial password set by manufacturers when hardware or software is delivered.

E

• **End user**: A user who employs computers acting as the source or destination of information flowing through a computer system.
• **External parties**: Non GS/OAS users or GS/OAS entities directly involved in a transaction or agreement with GS/GS/OAS. This includes external auditors, contractors and third parties.

F

• **File**: A set of related electronic records kept together.
• **Firewall**: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

G

• **GS/OAS Users**: Users of GS/OAS Network, working as staff, consultants (CPRs), associates, volunteers, interns, or any other type of work agreement with GS/OAS.

I

• **ID**: See Username.
**L**

- **Logon banner**: The initial message presented to a user when he/she connects to a computer.

**M**

- **Multi-user computer system**: Any computer system that can support more than one user simultaneously.

**O**

- **OAS-SDF**: OAS Software Development Framework
- **Organizational data**: Data related to GS/OAS activities stored in OAS production servers.

**P**

- **Password reset**: The assignment of a temporary password.
- **Password**: A string of characters that allows someone access to a computer system.
- **Personal data**: Non-work related data stored in the end user assigned workstation.
- **Privilege**: The special right to perform a certain action on a computer, such as read a specific computer file.
- **Privileged user ID**: A user ID that has been granted the ability to perform special activities, such as shut down a multi-user system.

**R**

- **Relevant External Parties**: Non GS/OAS users or GS/OAS entities directly involved in a transaction or agreement with GS/GS/OAS. This includes external auditors, contractors and third parties.
- **Restricted area**: An area where organizational data is processed and/or stored, or an area housing utilities or service facilities supporting organizational information equipment.
- **Router**: A device that forwards data packets to the appropriate parts of a computer network.

**S**

- **Sensitive information**: Restricted access information, the disclosure of which could damage the GS/GS/OAS and/or the GS/OAS. See Confidential Information.
- **Shared password**: A password known by or used by more than one user.
- **SLA**: Service Level Agreement
- **Software macro**: A computer program containing a set of procedural commands to achieve a certain result.
- **Special system privilege**: Access system privileges permitting a user or process to perform activities that are not normally granted to other users.
- **Suspending a user ID**: The process of revoking the privileges associated with a user ID.
• **System administrator:** In a multi-user computer system, is the role responsible for performing the functions in administrative operations and administrative reviews.

• **Third party:** From an Information Technology (IT) point of view, an organization (other than DOITS) or a person (not a staff member of DOITS or not hired by DOITS), that performs work or provides a product or service.

• **Top management:** The highest ranking GS/OAS functionaries - Secretary General, Assistant Secretary General, Chief of Staff, Secretaries, and Directors - who have the responsibility for and control of the General Secretariat.

• **User:** Person who uses computer or Internet services.

• **Username:** Is a character string that uniquely identifies a computer user or process. Also known as account or ID.

• **Working data:** Organizational data temporarily stored in the end user assigned workstation.
17 Annex 2 – Referenced Documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive order 09-1</td>
<td><a href="http://www.oas.org/legal/spanish/gensec/EXOR0901.htm">http://www.oas.org/legal/spanish/gensec/EXOR0901.htm</a></td>
</tr>
<tr>
<td>Checklist of Documents and Property to be Returned by Staff Members prior to Separation</td>
<td><a href="http://oasconnect/Portals/0/Forms/SeparationChecklistFormHeadquarters.doc">http://oasconnect/Portals/0/Forms/SeparationChecklistFormHeadquarters.doc</a></td>
</tr>
<tr>
<td>GS/OAS DOITS SLAs</td>
<td>To be done</td>
</tr>
<tr>
<td>Staff Rules</td>
<td><a href="http://www.oas.org/legal/english/rules/chapter1.htm">http://www.oas.org/legal/english/rules/chapter1.htm</a></td>
</tr>
</tbody>
</table>