



Indian Health Service Division of Information Security

OIT Guidelines on Navigating IHS Security Program Web Pages

GL 05-04

April 2005

FOR OFFICIAL USE ONLY

This information is intended for IHS use only. Disclosure is not expected to cause serious harm to IHS, and access is provided freely to all internal users via the organization's Intranet.

DOCUMENT INFORMATION

REVISIONS/RESCISSIONS

None

AUTOMATIC RESCISSION DATE

None

REVIEW

This guideline will be reviewed annually to maintain its currency and will expire in three years from the date of its approval.

EXCEPTIONS TO THIS GUIDELINE

None

TABLE OF CONTENTS

1.0 RECORD OF CHANGES..... 1

2.0 INTRODUCTION..... 2

3.0 USING THE IHS SECURITY WEB SITE..... 3

 3.1 Menu Bar 5

 3.2 Procedures 6

 3.2.1 Understanding the Procedures Page 6

 3.2.2 Accessing the Procedures Page 7

 3.3 Guidelines..... 8

 3.3.1 Understanding the Guidelines Page..... 8

 3.3.2 Accessing the Guidelines Page..... 9

 3.4 Forms..... 9

 3.4.1 Understanding the Forms Page 10

 3.4.2 Accessing the Forms Page 11

1.0 Record of Changes

Change No.	Date	Subject	Page No.
1	04/05/05	Finalized	NA

2.0 Introduction

This document is a user's navigation guide to using the IHS Security Program Web pages. It is a sample taken as of April 2005, therefore, the actual content of the pages at the time of reading this document may vary some but the main structure should remain very similar.

The IHS Security Team (IST) maintains these pages with assistance from the Web Team. It is intended to bring together all facets of the IHS Security Program into one location to provide various types of users the information they need about security to perform their jobs on a daily basis. Some of the links on the IHS Security pages link to other pertinent IHS documents such as the Indian Health Manual which is the policy of the IHS, not just Information Technology policy but policy governing all facets of the Indian Health Service. One will also find links to pertinent Department of Health and Human Services policy, procedures, and guidelines. To make searching easier for the user, IST has also provided links to other important security information and regulation. Users are encouraged to make comments and suggestions for the IHS Security Program Web pages so that IST can provide the maximum benefit for its users. You can contact the IHS Security Team by sending an e-mail to ITSCSecurity@IHS.gov.

Those users who have been designated as having significant security responsibilities should visit these pages often for updates, Standard Operating Procedures issued for a review and comment and other significant security information necessary to carry out their security responsibilities.

Security documents that are considered to contain information that may cause potential harm to the agency if their contents were released publicly (i.e., outside of IHS) will not be posted on these Web pages. They will be available by request to any user who has a demonstrated business need to know. It is understood that items provided on this Web site carry the following disclaimer: *For Official IHS and HHS Use only. This information is intended for HHS/IHS, use only. Disclosure is not expected to cause serious harm to HHS/IHS, and access is provided freely to all internal users via IHS Intranet.*

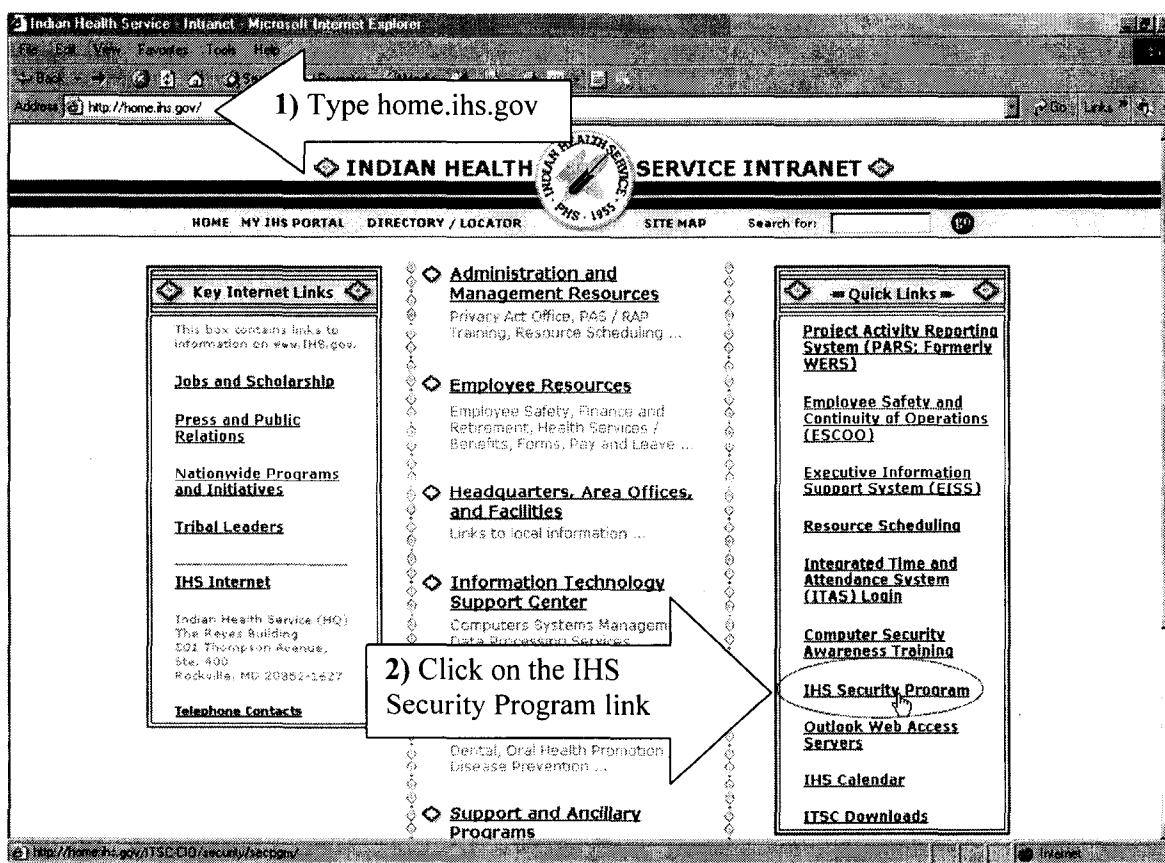
3.0 Using the IHS Security Web Site

Follow these steps to access to IHS Security Web site

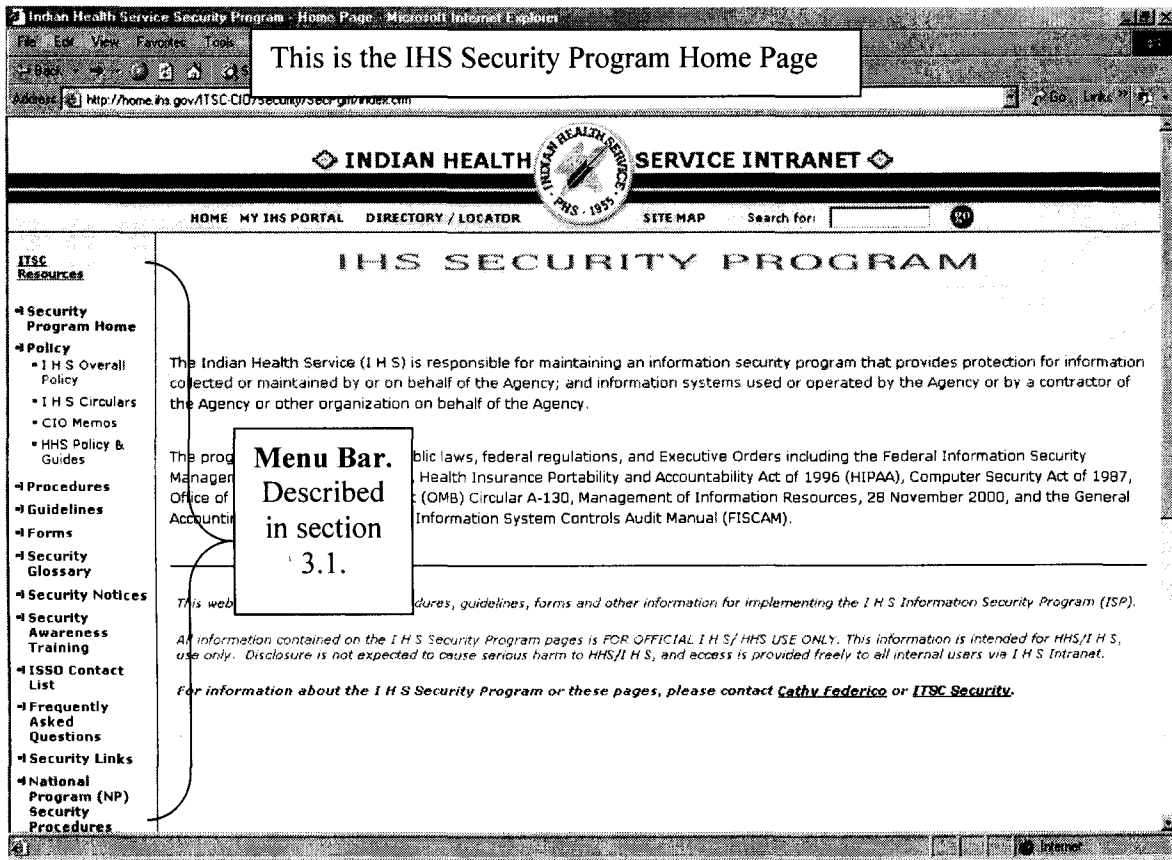
1. Point the chosen internet browser to <http://home.ihs.gov>.
2. Click on the **IHS Security Program** link located on the right side of the page in the Quick Links box.

Or

3. Use the direct address: <http://home.ihs.gov/ITSC-CIO/security/secpgm/>.



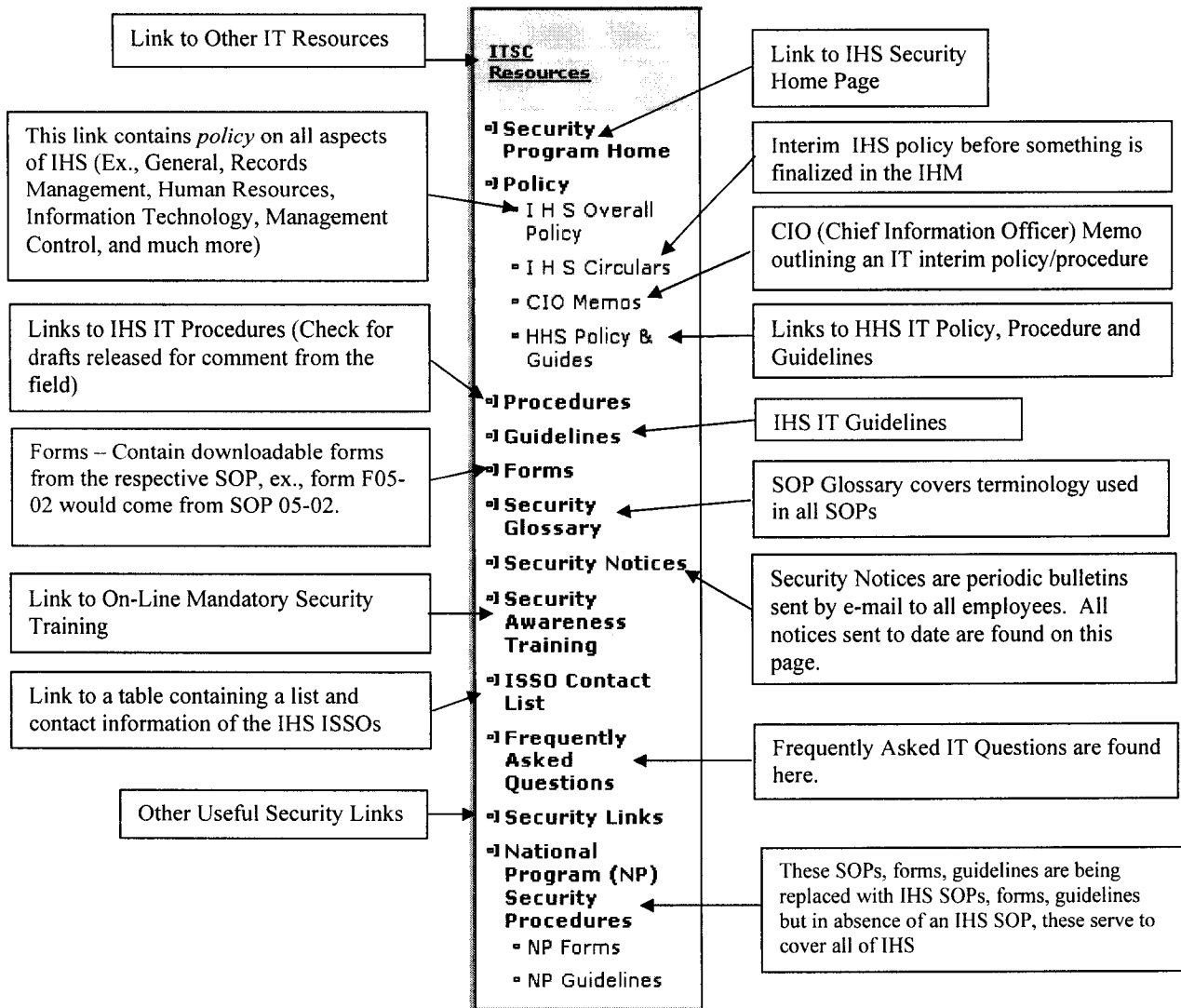
4. The IHS Security Program home page will display, as shown below. The home page is the main page of the Web site. The home page serves as an entrance and introduction to the site.



Sections 3.1 through 3.4 explain the menu bar, main IHS Procedures page, Guidelines page, and Forms page. Each page is explained with screen captures with descriptions on how to read the page.

3.1 Menu Bar

A menu bar is a menu arranged horizontally or vertically on a Web site. Each page of the Security Web site will have the menu bar displayed on the left side of the screen. The menu bar allows you to easily move around the Security Web site by simply clicking on any of the links. Each of the links are described below.

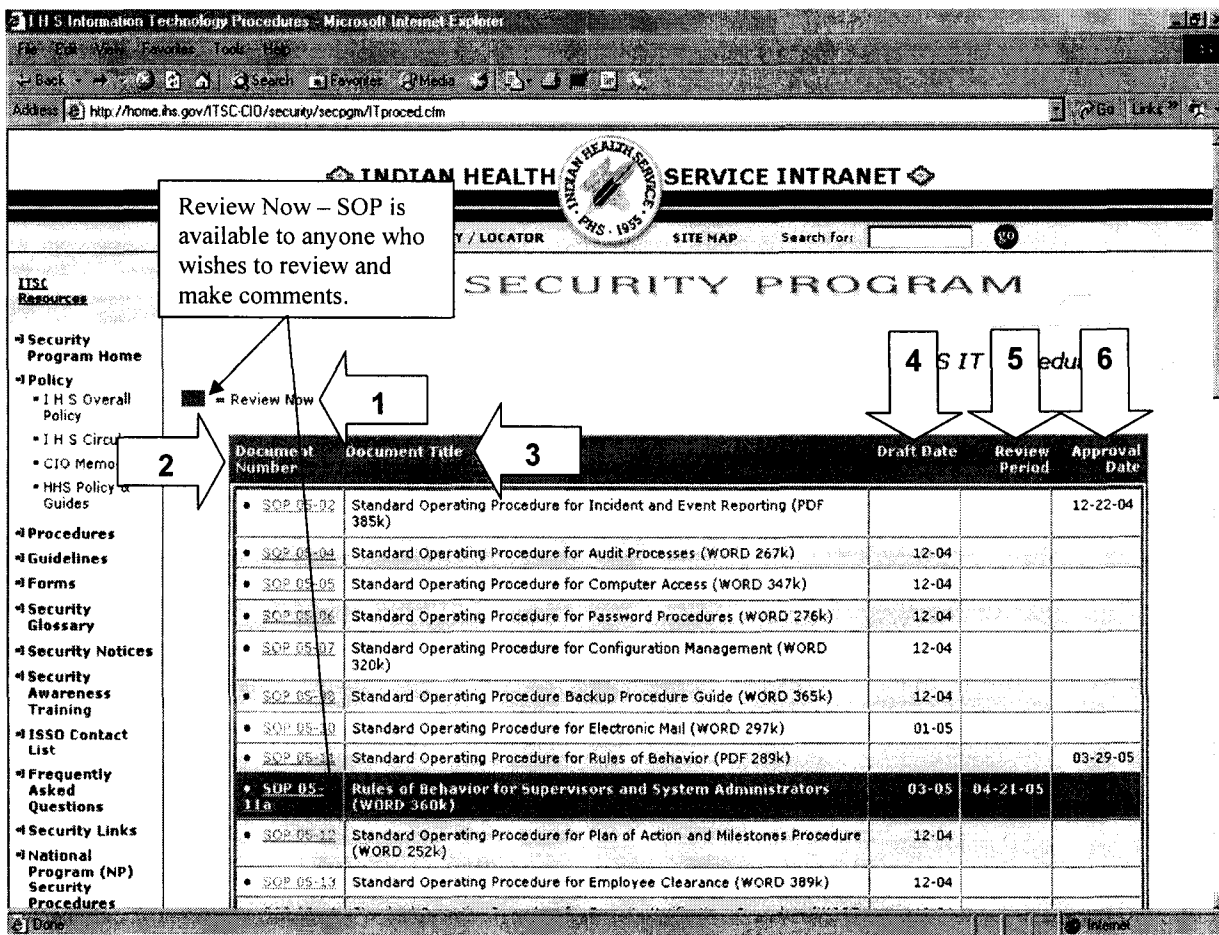


3.2 Procedures

The Procedures page, contains a table of all the Information Technology (IT) Standard Operating Procedures (SOP).

3.2.1 Understanding the Procedures Page

Below is a screen capture of the Procedures page. Each of the arrows identifies a column which is explained by the arrow's corresponding number below the screen capture.



- 1. Review Now:** SOP is available to anyone who wishes to review and make comments.
- 2. Document Number:** Example SOP 05-16: SOP (Standard Operating Procedure), 05 stands for year updated, 16 is the procedure number.
- 3. Document Title:** Name of the SOP and basic topic area covered in the SOP

4. **Draft Date:** Date of the most recent SOP draft
5. **Review Period:** Closing Date of Peer Review of Draft (Must provide comments to ITSC Security by closing date). Please provide these comments to the IHS Security team by sending an e-mail to ITSCSecurity@IHS.gov.
6. **Approval Date:** Date of Final Approved SOP for IHS implementation. Note that all SOPs will be reviewed at least annually.

3.2.2 Accessing the Procedures Page

To access the Procedures Web page, click on the **Procedures** link from the IHS Security Program home page. You can also directly access this page by entering <http://home.ihs.gov/ITSC-CIO/security/sepqgm/ITproced.cfm> into your Web browser.

The screenshot shows two overlapping browser windows. The top window displays the 'INDIAN HEALTH SERVICE INTRANET' header and the 'IHS SECURITY PROGRAM' main heading. A left-hand navigation menu includes links for 'Procedures', 'Guidelines', 'Forms', 'Security Glossary', 'Security Notices', 'Security Awareness Training', 'ISSO Contact List', 'Frequently Asked Questions', 'Security Links', and 'National Program (NP) Security Procedures'. A large white arrow points from the 'Procedures' link in the menu to the 'IHS IT Procedures' page in the bottom window.

The bottom window shows the 'IHS IT Procedures' page with a table of documents. The table has columns for Document Number, Document Title, Draft Date, Review Period, and Approval Date. The following table represents the data shown in the screenshot:

Document Number	Document Title	Draft Date	Review Period	Approval Date
• SOP-05-02	Standard Operating Procedure for Incident and Event Reporting (PDF 385k)			12-22-04
• SOP-05-04	Standard Operating Procedure for Audit Processes (WORD 267k)	12-04		
• SOP-05-05	Standard Operating Procedure for Computer Access (WORD 347k)	12-04		
• SOP-05-06	Standard Operating Procedure for Password Procedures (WORD 276k)	12-04		
• SOP-05-07	Standard Operating Procedure for Configuration Management (WORD 320k)	12-04		
• SOP-05-08	Standard Operating Procedure Backup Procedure Guide (WORD 365k)	12-04		
• SOP-05-10	Standard Operating Procedure for Electronic Mail (WORD 297k)	01-05		
• SOP-05-11	Standard Operating Procedure for Rules of Behavior (PDF 289k)			03-29-05
• SOP-05-11A	Rules of Behavior for Supervisors and System Administrators (WORD 368k)	03-05	04-21-05	
• SOP-05-12	Standard Operating Procedure for Plan of Action and Milestones Procedure (WORD 252k)	12-04		
• SOP-05-13	Standard Operating Procedure for Employee Clearance (WORD 389k)	12-04		

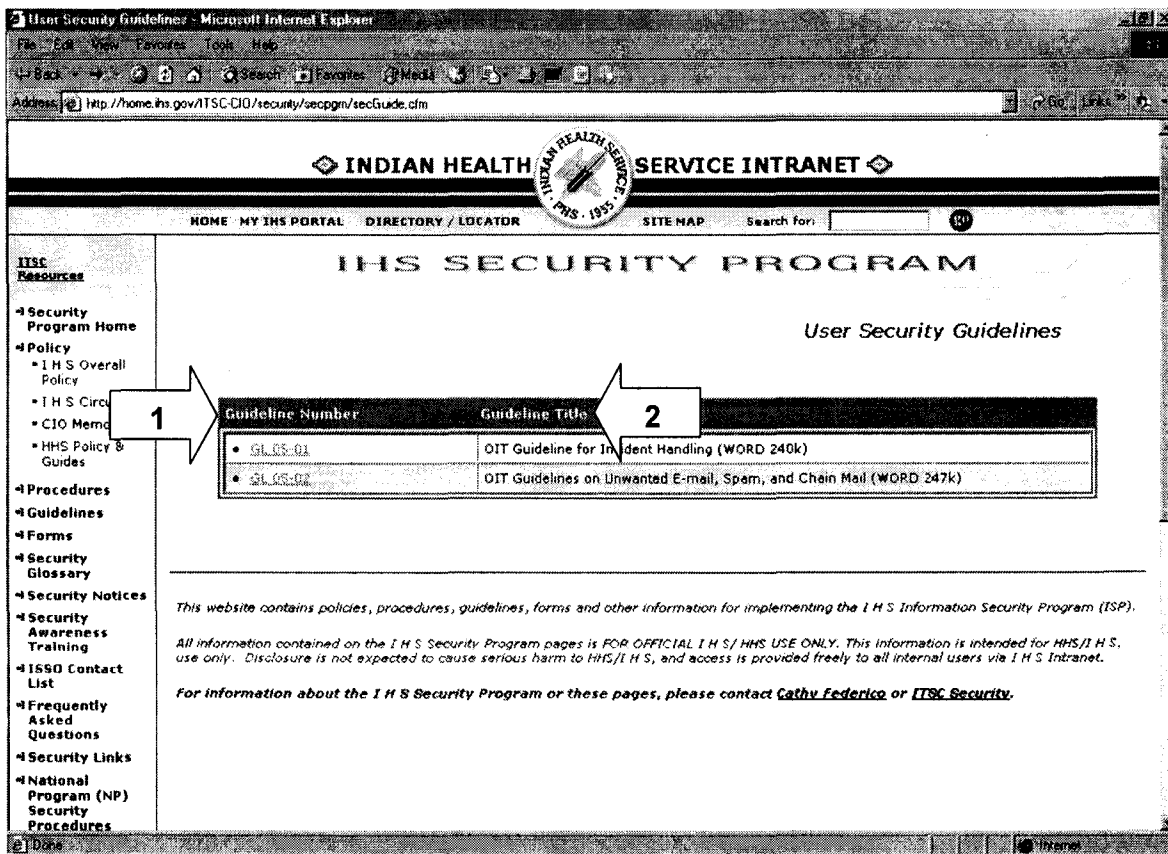
3.3 Guidelines

Guidelines are supplemental information to policy, SOPs, or other IT directives. These are not considered policy but are highly suggested that they be implemented across the agency.

3.3.1 Understanding the Guidelines Page

Below is an example from the IHS Information Technology (IT) Guidelines page (<http://home.ihs.gov/ITSC-CIO/security/secpgm/secGuide.cfm>).

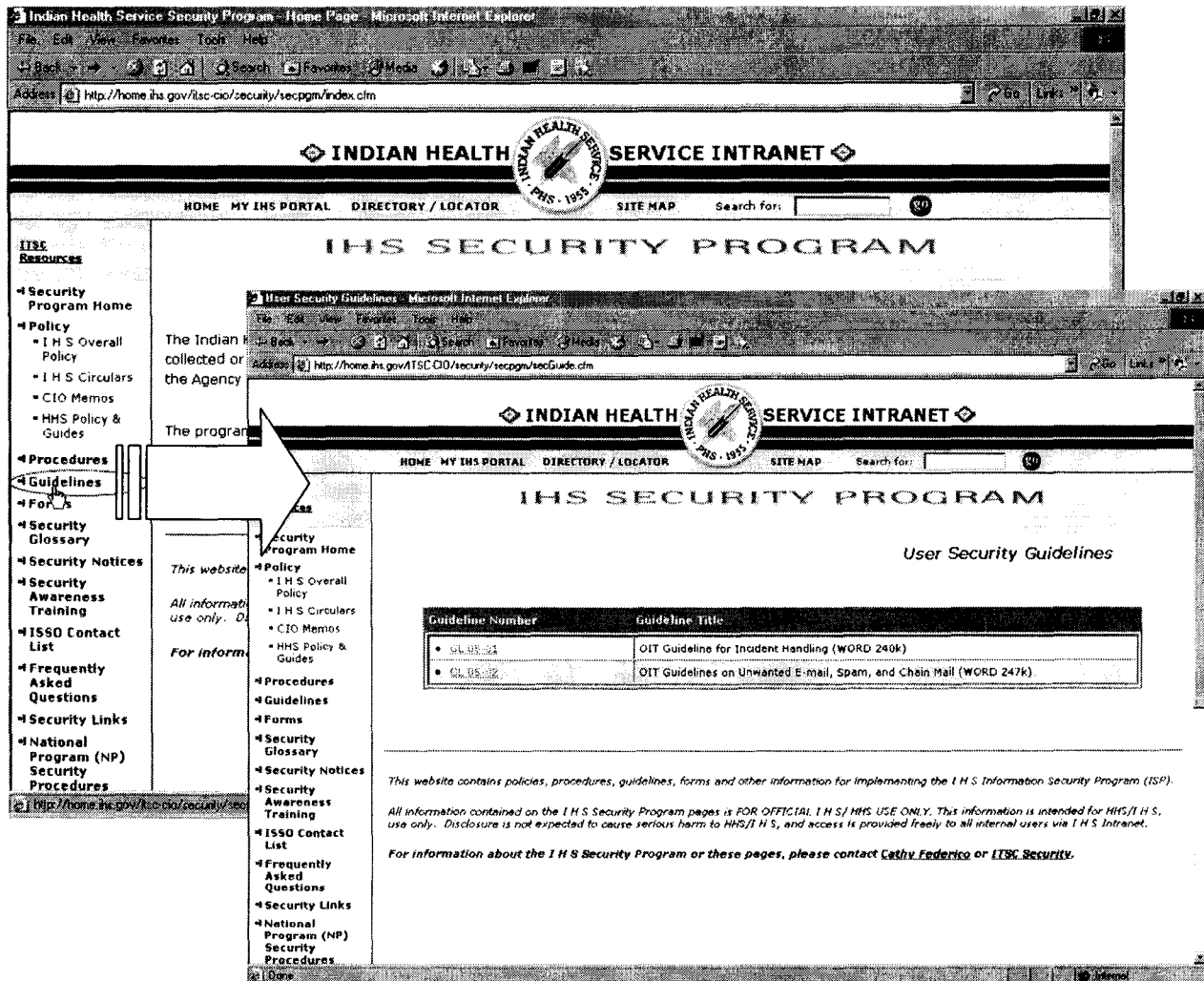
Each of the arrows identifies a column which is explained by the arrow's corresponding number below the screen capture.



1. **Guideline Number:** This is the official guideline number. GL indicates that the document is a guideline. The 05 stands for year updated, 01 is the guideline number.
2. **Guideline Title:** Name of the guideline and basic topic area covered.

3.3.2 Accessing the Guidelines Page

To access the Guidelines Web page, click on the **Guidelines** link from the IHS Security Program home page. You can also access the page by entering <http://home.ihs.gov/ITSC-CIO/security/secpgm/secGuide.cfm> directly into your Web browser.



3.4 Forms

These are downloadable copies of any form found in the respective SOP on the subject. Please note that besides being an SOP and a Form, there may also be applicable Guidelines.

3.4.1 Understanding the Forms Page

Below is an example from the IHS Information Technology (IT) Forms page (<http://home.ihs.gov/ITSC-CIO/security/secpgm/secForm.cfm>). Each of the arrows identifies a column which is explained by the arrow's corresponding number below the screen capture.

The screenshot shows the IHS Security Program web page. The main heading is "IHS SECURITY PROGRAM" with the subtitle "I H S Security Forms". A table titled "I H S Security Forms" is displayed with three columns: "Form Number", "Form Title", and "Related SOP". Three arrows point to these columns, labeled 1, 2, and 3 respectively.

Form Number	Form Title	Related SOP
F05-02a	Monthly Security Events (EXCEL 15k)	05-02
F05-02k	IHS Incident Reporting Form (EXCEL 17k)	05-02
F05-03	Security Reporting Template (EXCEL 62k)	05-03
F05-05	Request for Computer Access Form (PDF 158k)	05-05
F05-07	Configuration Management Change Request Form (PDF 49k)	05-07
F05-13a	Clearance HHS 419 Form (PDF 76k)	05-13
F05-13k	Clearance Circular Exhibit 2002-6-A (PDF 73k)	05-13
F05-16	Web Site Request Form (PDF 101k)	05-16
F05-22	Physical Access Form (PDF 57k)	05-22
F05-26	Removal of Data and Software (PDF 37k)	05-26
F05-27	Interconnection Security Assessment Template (PDF 59k)	05-27
F05-29	DNS Request Form (PDF 29k)	05-29

- 1. Form Number:** This is the official form number. The form number relates back to the related SOP. Example: F05-02a would be the Monthly Security Events Report form from SOP 05-02 Standard Operating Procedure for Incident and Event Reporting. The "F" indicates that the document is a form. The 05 stands for year updated, 01 is the form number.
- 2. Form Title:** Name of the form and basic topic area covered.
- 3. Related SOP:** This is the SOP to which the form is related.

3.4.2 Accessing the Forms Page

To access the Forms Web page, click on the **Forms** link from the IHS Security Program home page. You can also access the page by entering <http://home.ihc.gov/ITSC-CIO/security/secpgm/secForm.cfm> directly into your Web browser.

The screenshot shows two overlapping browser windows. The top window displays the 'IHS SECURITY PROGRAM' home page with a navigation menu on the left. The bottom window shows the 'IHS Security Forms' page, which contains a table of security forms. A white arrow points from the 'Forms' link in the left-hand navigation menu of the top window to the 'Forms' link in the left-hand navigation menu of the bottom window.

IHS Security Forms

Form Number	Form Title	Related SOP
• FDS-220	Monthly Security Events (EXCEL 15k)	05-02
• FDS-221	IHS Incident Reporting Form (EXCEL 17k)	05-02
• FDS-222	Security Reporting Template (EXCEL 62k)	05-03
• FDS-223	Request for Computer Access Form (PDF 158k)	05-05
• FDS-224	Configuration Management Change Request Form (PDF 49k)	05-07
• FDS-225	Clearance HHS 419 Form (PDF 76k)	05-13
• FDS-226	Clearance Circular Exhibit 2002-6-A (PDF 73k)	05-13
• FDS-227	Web Site Request Form (PDF 101k)	05-16
• FDS-228	Physical Access Form (PDF 57k)	05-22
• FDS-229	Removal of Data and Software (PDF 37k)	05-26
• FDS-230	Interconnection Security Assessment Template (PDF 59k)	05-27
• FDS-231	DNS Request Form (PDF 29k)	05-29

Martin, R. Frank

From: Federico, Kathleen (OIT)
Sent: Wednesday, April 06, 2005 11:20 AM
To: Federico, Kathleen (OIT); IHS ALL
Subject: RE: IHS Security Program Web Page Navigation Guide

If this is a duplicate, accept my apologies. Attachment – Navigation Guide - included.

Cathy Federico

Think about *how you can*, rather than *why you can't*

Asst. ISSO

Phone: 505-248-4381

Cell: 505-975-4230

Fax: 505-248-4199

Focus on the process not on blame

This email may contain confidential and/or privileged information. If it is evident that you are not the intended recipient, please notify the sender immediately and destroy this email.

Unauthorized copying, disclosure, or distribution of the material in this email is strictly forbidden.

From: Federico, Kathleen (OIT)
Sent: Tuesday, April 05, 2005 4:46 PM
To: IHS ALL
Subject: IHS Security Program Web Page Navigation Guide

Attached please find a guideline for navigating the IHS Security Program website located on <http://home.ihs.gov>.

This site is where IHS posts information pertaining to information security. On this site you will find links to:

- Indian Health Service (IHS) Manual (covers Indian Health Service Policy for the agency, not just IT)
- IHS Circulars
- IHS IT Policy and Procedure (Standard Operating Procedures (SOP))
- IHS Computer Security Notices (the ones I send out by mail and then post to intranet)
- IHS IT Guidelines (relating to security)
- IHS IT Forms (relating to security including computer access, incident reporting, etc.)
- IT Glossary of Terms
- IHS Computer Security Awareness Training
- HHS Policy and Procedure pertaining to IT
- Listing of IHS Information Systems Security Officers (ISSO)
- Other Security Links

All employees (users) should become familiar with the IHS Security Program pages and their contents.

Cathy Federico

Security is NOT a one time process. It is NOT an IT problem; it IS a BUSINESS problem

Asst. ISSO

4/6/2005

Phone: 505-248-4381

Cell: 505-975-4230

Focus on the process not on blame

This email may contain confidential and/or privileged information. If it is evident that you are not the intended recipient, please notify the sender immediately and destroy this email. Unauthorized copying, disclosure, or distribution of the material in this email is strictly forbidden.

4/6/2005