Minimum Security Requirements for Public Websites of the United Nations ICT Technical Procedure

Ref: SEC.03.PROC

Revision History

Serial Number	Release Description	Release Number	Release Date	Author(s)
1.	Endorsed by the ICT Policy Committee	1.0	6 December 2013	Endorsed by the ICT Policy Committee
2.	Approved by CITO	1.0	9 December 2013	Atefeh Riazi, ASG/CITO
3.	Scheduled revision by the ICT Policy Committee. Changes: - Added "Overview" section - Added "Section 1: Purpose and Scope" - Added "Section 2: Responsibilities" - Replaced "shall" with "must" for "baseline" requirements under Section 3. - Other small edits for correction or clarification - Added Section 4 "Ongoing Revisions"	2.0	17 March 2017	Revision endorsed by the ICT Policy Committee

Approved By

Atefeh Riazi, ASG/CITO

Date: 4/April/ 2017

Minimum Security Requirements for Public Websites of the United Nations ICT Technical Procedure[1]

Overview

- Public websites (directly accessible from the Internet) are inherently vulnerable to various types of attacks and, therefore, require at a minimum some basic security measures. Attacks against websites can be classified as follows:

  (a) *Availability attacks*: including Denial of Service (DoS), and destruction of websites or their content.

  (b) *Integrity attacks*: such as attempts to modify the content of a website, either visibly ("defacement"), or by adding or embedding malicious software or code in order to negatively affect subsequent visitors of the site.

  (c) *Confidentiality attacks*: unauthorized access to sensitive data, such as information about users, including email addresses and access credentials.

- In addition, a compromised public website can also be used to host malware and/or illegal content, or as a stepping stone to attack the Organization's internal network or that of a partner organization.

- Website vulnerabilities that could be exploited by attacks include:

  (d) Known vulnerabilities in the underlying third-party software (operating systems, web servers, databases, web content management frameworks, etc.),

  (e) Vulnerabilities in the specific code developed for the site, and/or

  (f) Social engineering, by tricking website administrator or users with elevated access rights to modify configuration/parameters that can then be exploited.

Section 1

Purpose and Scope

1.1 The purpose of this procedure is to establish minimum security requirements for United Nations websites. It defines a baseline of the most essential controls that must be implemented on any website of the United Nations as a matter of urgency.

[1] The controls defined in this technical procedure are based on recommendations of an inter-agency working group operating under the Chiefs Executives Board.

1.2 This policy applies to all websites that are directly accessible from the Internet and are maintained and/or operated by or for any department or office of the United Nation Secretariat, including those away from Headquarters, as well as missions and information centres ("author departments", as defined in ST/AI/2001/5 "United Nations Internet publishing").

1.3 This document shall be read in conjunction with ST/AI/2001/5 "United Nations Internet publishing, information security policies, and other ICT policies and guidelines available on the UN intranet (iseek.un.org/department/policies)

1.4 The controls mandated by this procedure provide only a minimum baseline that is mandatory for all types of websites. In many cases, additional controls will be required to adequately protect complex "web applications" or websites that contain sensitive information. The Office of Information and Communications Technology can assist with the assessment of requirements and advise on specific controls. Additional controls may include "Best practice" guidelines and checklists for web application security, which are available from many software vendors and distributors, as well as community organizations dedicated to this topic.

Section 2

Responsibilities

2.1 All Secretariat organizational entities - including ICT service providers, departments and offices - that maintain, or plan to establish one or more websites, have the responsibility to ensure that all applicable controls described in this Procedure are implemented on all websites that they own, maintain and/or operate.

2.2 The Office of Information and Communications Technology is mandated to verify the effective implementation of these minimum requirements. Where non-compliance of a website is determined to pose an operational or reputational risk to the Secretariat, access to the website will be limited until any missing or insufficient controls have been implemented.

2.3 Where third parties are involved in the development, maintenance or hosting of a website, the list of required controls listed in this Technical Procedure should be included as a mandatory element in any related contract.

2.4 As DoS attacks typically originate from a multitude of locations, they are best mitigated at the network level. Internet Service Providers (ISPs) are typically in the best position to provide this service. The operators of "high profile" websites that are likely to become the target of such DoS attacks should therefore include the protection against such attacks in the service contract with their respective ISPs.

Section 3

ICT Technical Procedure

Baseline for all public websites of the United Nations

3.1 All websites must have an assigned and accountable owner, and be registered with the Office of Information and Communications Technology. At the time of registration the responsible department or office must indicate the level of compliance, and in the case of partial compliance include a plan describing the steps and time frame required to achieve compliance with this instruction.

3.2 All components (web server(s), database(s) and other back-end server(s), web content management framework, etc.) must be configured according to the relevant vendor/distributor security recommendations and internal practices and policies of the United Nations Secretariat. This statement includes the requirement to change the (default) passwords for all pre-defined accounts, and to use strong passwords that are compliant with Organization's password policy

3.3 All applicable security updates ("patches") must be assessed within 30 days and acted upon accordingly.

3.4 Databases and other back-end systems may be accessed only indirectly through the web application, and must not be made directly accessible from the Internet. Only the services that are required for the site's functionality may be made accessible.

3.5 All connections from web application front-ends to back-end systems must be configured to use minimal privileges. Processes on the servers must run with minimal privileges. When feasible, database service accounts must only be able to read, not update, content. "Write" access must be limited to the database table that is being updated.

3.6 All user-provided input must be validated before it is passed on to back-end systems or returned to the user. Input must be validated against its type (string, number, date, etc.), range (e.g. positive integers), size (number of characters), valid syntax or set of valid responses (e.g. in drop down lists). Invalid input must either be rejected or "sanitized" by removing or safely encoding any invalid elements from the user-provided input.

3.7 Websites that allow uploading of files (images, documents, etc.) must verify the file type and, where possible, be scanned for malicious code.

3.8 Web applications must not display error or system messages that reveal information about the underlying configuration.

3.9 Information that is not necessary for the functioning of the web server must be removed or moved to a more secure location. Components (widgets, plugins, add-ons, etc.) that are not necessary for the functioning of the web server must be disabled or uninstalled. Any component that is essential for the functioning of the website must be tested for vulnerabilities, approved and regularly maintained and updated.

3.10 Relevant activity on the server and in the application must be monitored and tracked by appropriate logging mechanisms for auditing and accountability purposes, according to the policies of the United Nations Secretariat (see: System Monitoring and Log Management TP). The generated information must be secured against tampering and retained according to applicable retention policies (see: Retention Schedule for ICT Records TP).

3.11 Access with elevated access rights (e.g. for maintenance or administration purposes) must be protected, e.g. using two-factor authentication or limiting access to specific locations.

Additional controls for websites that allow or require users to login

The following additional requirements apply to all websites that allow or require users to login:

3.12 All sites must use the "secure hypertext transfer protocol" (HTTPS) to ensure that user credentials and other potentially confidential content cannot be intercepted during transmission. HTTPS uses secure socket layer certificates to verify the authenticity of a website and encrypt all communications between the user and the website. Certificates must be (a) issued by a vendor that is automatically recognized as "trusted" by major browsers, (b) replaced before their expiration date, and (c) utilize secure cryptographic ciphers and keys.[2]

3.13 Passwords must not be stored in "clear text", but in a form that protects them even in case of a compromise. This implies that the "send my password" functionality is not possible, only the "send a link to change password" is possible.

3.14 Users shall be able to change their password without intervention of another person.

3.15 Controls that prevent brute-force attacks against user accounts must be implemented, e.g. by "locking out" accounts after a pre-defined number of invalid login attempts, or by displaying a CAPTCHA test (or alternative mechanisms) to prevent automated login attempts

3.16 Users shall only be able to access content for which they possess specific authorization.

3.17 Authenticated users shall be able to log out. All sessions shall be maintained by the web server in a secure manner. Sessions must be maintained using the controls of the web content management framework. The session id must be generated randomly at logon (i.e. not be guessable), long enough to prevent brute-force attacks (e.g. 20 characters or longer), and not be disclosed in the URL. Sessions must be invalidated when the user logs out, terminated after a pre-defined period of inactivity, and set to automatically expire after a maximum amount of time regardless of activity.

[2] OICT has contracted with a third party vendor to issue such certificates. Details of this service as well as instructions on how to requests certificates are provided at https://iseek.un.org/departmental_page/ssl-certificates-2016-2017

Section 4

Ongoing Revisions

4.1 This ICT Technical Procedure must be reviewed by the ICT Policy Committee:

a) on an ongoing basis, at least once a year

b) after a major internal security incident has taken place

c) upon major changes to the United Nations internal network architecture

--- End of Document ---