



INTERNAL AUDIT DIVISION

REPORT 2023/102

Audit of management and security of websites and social media in the United Nations Secretariat

**The Secretariat needs to implement
mechanisms institutionalizing the use of
social media and management of websites
effectively and securely**

**29 December 2023
Assignment No. AT2022-580-01**

Audit of management and security of websites and social media in the United Nations Secretariat

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of management of websites and social media in the United Nations Secretariat. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the management of websites and social media accounts in the Secretariat. The audit covered the period from January 2021 to June 2023 and covered risk areas related to websites and social media which included: (a) governance and policy framework for social media; (b) governance and policy framework for websites; (c) content management; (d) security of websites and social media; and (e) information and communications technology support.

The audit indicated the need for the Secretariat to implement mechanisms institutionalizing the use of social media and management of websites effectively and securely.

OIOS made 10 recommendations. To address the issues identified in the audit, the Department of Global Communications (DGC) needed to:

- Strengthen the framework for governance and management of social media in the Secretariat by developing guidelines for Secretariat entities on strategies and use of social media in furtherance of their mandates, and establishing a committee or similar body for coordination and review of the social media needs of the Secretariat;
- Undertake an annual campaign to ensure the upkeep and completeness of the social media database in accordance with the Secretary-General's bulletin on the institutional use of social media in the Secretariat;
- In coordination with the Office of Information and Communications Technology (OICT) and the respective Secretariat entities, work to raise the awareness of and requirements for compliance with website governance;
- Assign resources to ensure compliance with the website accessibility standards for the Organization's public websites;
- In coordination with OICT, undertake a capacity assessment and establish a process for decommissioning websites in accordance with ST/AI/2022/2;
- Define guidelines for the use of multi-factor authentication across social media accounts; and
- Assess the requirements for automated tools to monitor the Secretariat's websites and social media accounts.

OICT needed to:

- Establish a process for periodic independent security assessment for the Secretariat's websites with a focus on remediation of the already identified ICT security vulnerabilities;
- In coordination with DGC and other Secretariat entities, finalize the protocol of the hybrid cyber security response team with clear terms of reference, roles and responsibilities, and actionable timelines; and
- In coordination with DGC, prioritize the implementation of the integrated web communications platform to improve compliance with website publishing standards and address the presently fragmented web presence.

DGC and OICT accepted nine recommendations. Actions required to close these recommendations are indicated in Annex I. However, DGC did not accept one recommendation related to assigning resources to ensure compliance with website accessibility standards for the Organization's public websites. OIOS notes that compliance with website accessibility standards by the Organization's public websites is required for providing accessibility to persons with disabilities. This unaccepted recommendation has been closed based on Management's acceptance of the residual risks.

CONTENTS

I. BACKGROUND	1
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	1-2
III. AUDIT RESULTS	2-13
A. Governance and policy framework for social media	2-5
B. Governance and policy framework for websites	5-7
C. Content management	7-9
D. Security of websites and social media	10-11
E. ICT support	12-13
IV. ACKNOWLEDGEMENT	13
ANNEX I	Status of audit recommendations
APPENDIX I	Management response

Audit of management and security of websites and social media in the United Nations Secretariat

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of management and security of websites and social media in the United Nations Secretariat.
2. The Department of Global Communications (DGC) informs the public, civil society and Member States with information and communicates the United Nations' story around the world through its global networks. DGC is supported by United Nations Information Centres (UNICs) worldwide, comprising 59 field offices covering 139 countries. DGC provides the policy framework for institutionalizing the use of social media¹ and management of websites and website publishing. However, entities within the Secretariat are responsible for managing their websites and social media platforms in conformance with the policy framework established by DGC and the technical standards established by the Office of Information and Communications Technology (OICT).
3. The Secretariat entities' communications portfolio consists of more than 760 public websites and 450 social media accounts on various platforms. For example, UNICs maintained a portfolio of 109 websites in local and official languages and 303 social media accounts in thirty languages across seven major platforms.
4. DGC has made efforts to regulate the management of websites and social media in the Secretariat in terms of ST/AI/2022/2 on United Nations website publishing. Similarly, DGC led the formulation of the Secretary-General's bulletin ST/SGB/2019/5 on institutional use of social media² which provides a legal and operational framework governing the institutional use of social media by authorized staff members.
5. DGC's Social Media Section manages the flagship social media accounts of the Secretariat and also: (i) helps manage the Organization's relationship with major social media platforms including Facebook, Instagram, LinkedIn, Snapchat, X, WeChat and Weibo; (ii) develops policies and guidelines for the use of social media platforms by the United Nations; and (iii) provides social media guidance and support to United Nations officials and Member States.
6. OICT establishes the technical standards for information security in the Secretariat and provides support for development and hosting of selected websites. It is responsible for maintaining the website registry and dashboard for compliance with the standards for website publishing.
7. Comments provided by DGC and OICT are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

8. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the management of websites and social media accounts in the Secretariat.

¹ Social media accounts can be categorized as microblogs (e.g., Twitter - now X), image sharing (e.g., Flickr and YouTube), social network sites (e.g., Facebook), professional networking sites (e.g., LinkedIn) and Instant messaging (e.g., Snapchat).

² Institutional social media accounts are accounts on social networking platforms that are authorized by and belong to an entity of the Secretariat for official purposes. The definition does not include personal social media accounts of United Nations staff members and staff representative bodies.

9. This audit was included in the 2022 risk-based work plan of OIOS due to risks associated with the management of websites and social media in the Secretariat.

10. OIOS conducted this audit from February to July 2023. The audit covered the period from January 2021 to June 2023. Based on an activity-level risk assessment, the audit covered risk areas related to websites and social media which included: (a) governance and policy framework for social media; (b) governance and policy framework for websites; (c) content management; (d) security of websites and social media; and (e) information and communications technology (ICT) support.

11. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) walkthroughs; (d) analytical review of data; and (e) ICT security tests. The audit reviewed public websites and the iSeek intranet. The audit did not review web applications and interactive web portals requiring user authentication and interaction to carry out specific actions and tasks.

12. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

III. AUDIT RESULTS

A. Governance and policy framework for social media

Need for a social media strategy and framework for the Secretariat

13. Best practices require that organizations should develop a framework and strategy for the management of their social media accounts so that their mandates, work and communication can reach the targeted audience timely and securely. The framework should be supported with policies, ongoing risk assessments, communication strategies, brand protection, data management, technology support, tools and formalized forums for discussion and decision-making.

14. Social media use in the Secretariat is governed by the Secretary-General's bulletin ST/SGB/2019/5 on the institutional use of social media. OIOS noted the following:

(a) While DGC had documented a social media strategy ("Global Social Media Strategy-2021"), this document was meant for internal use of DGC and not for the Secretariat at large. The strategy states that DGC will continue to provide guidance on social practice and policy across the United Nations system. However, DGC had not issued guidance on social media practices to be adopted by Secretariat entities. Furthermore, the strategy did not cover all types of social media platforms, their governance, and branding.

(b) There was lack of a committee or other body in the Secretariat with oversight and coordination responsibilities for monitoring the current state of social media use, capability assessment, and the future direction for use of social media in the Secretariat.

(c) DGC and the Secretariat's entities had not conducted any assessment to determine current capabilities and resources for managing social media accounts and platforms. Such an assessment is key to formulating effective procedures for the use of social media. There was no guidance on social media adoption and the related platforms to be used, as well as content and communications requirements of individual entities. For instance, while DGC was present on 13 different social media platforms, the Department of Peace Operations was present on only seven platforms. Entities were operating their social media in isolation without an overall framework for coordination on the best use of social media.

(1) DGC should strengthen the framework for governance and management of social media in the Secretariat by: (a) developing guidelines for Secretariat entities on strategies and use of social media in furtherance of their mandates; and (b) establishing a committee or similar body for coordination and review of the social media needs of the Secretariat.

DGC accepted recommendation 1.

Need to monitor and manage the institutional use of social media

15. The Secretary-General's bulletin ST/SGB/2019/5 on the institutional use of social media only applies to institutional social media accounts that are authored by and belong to an entity of the Secretariat for official purposes. It does not include social media accounts created by United Nations staff and their representative bodies. OIOS noted the following:

(a) DGC maintained a central database listing all institutional social media accounts in the Secretariat. While Heads of Secretariat entities were responsible for keeping the database updated, there was no mechanism to ensure that the database remained up-to-date. There were 454 social media accounts registered in the database across 15 platforms, of which 343 were entered in the registry in 2019 without further updates. Only eight entries were recorded in 2022 and 2023. Further, some of the accounts were no longer active while others had a limited number of followers – such as Atavist (<https://dppa-ps.atavist.com/>) and Medium social media accounts (<https://unpeacekeeping.medium.com>). Similarly, one clubhouse account was no longer in use (<https://www.joinclubhouse.com/club/united-nations-technology>).

(b) The name of the respective account managers for Secretariat entities was not updated in the registry in all cases (e.g., alternate officer for <https://dppa-ps.atavist.com/>). OIOS could not confirm whether the social media registry had valid names and contact details in all cases. There was no procedure to ensure that information from these accounts was preserved. There was need to review the database at least annually to ensure that it is up-to-date. DGC stated that such an annual review would require additional resources.

(c) To establish an institutional social media account, Secretariat entities were required to demonstrate the need for such an account to avoid duplication. Similarly, establishing social media accounts required a risk analysis (reputational or security) to be done by the Heads of Secretariat entities. All these accounts were expected to be registered in the DGC database within 10 days of their creation. However, currently, there was no mechanism to ensure that these provisions of the Secretary-General's bulletin are complied with. The DGC database did not require Secretariat entities to upload documentation demonstrating compliance with the bulletin. Also, there was no guidance for conducting the risk analysis of social media accounts.

(d) The Secretary-General's bulletin requires that where feasible, Heads of Secretariat entities should take into consideration paragraph 36 of General Assembly resolution 69/325 in which the Assembly underlined the importance of implementing new communication tools such as social networks, and consideration of the linguistics dimension to assure parity among the six official languages of the Organization. OIOS' analysis of the social media registry showed that approximately 30 per cent of the accounts were in languages other than English, with many of them being in French and Spanish (50 per cent of non-English accounts). Additionally, these accounts were spread across 12 Secretariat entities and missions. There was no mechanism to track the number of non-English social media accounts across various entities to promote multilingualism effectively.

(2) DGC should undertake an annual campaign to ensure the upkeep and completeness of the social media database in accordance with the Secretary-General's bulletin on the institutional use of social media in the Secretariat.

Need to strengthen the Secretary-General's bulletin on institutional use of social media

16. OIOS noted that several important areas were not covered in the existing bulletin (ST/SGB/2019/5) on the institutional use of social media, including the following:

(a) Defining the purpose of social media accounts – Good practices recommend that organizations communicate the purpose of their institutional social media accounts on their websites to attract the right audience. The flagship website of the United Nations (<https://www.un.org/en/get-involved/social-media>) mentioned the main institutional social media platforms for departments, offices and entities without specifying the purpose for which these accounts were used. For example, the TikTok account of the United Nations had 174,000 followers with videos on several topics such as the Sudan war, clean water, climate change and gender equality. It was unclear how these posts related to each other and what the visitor could expect from this account.

(b) Leadership accounts – The Secretary-General's bulletin did not provide guidance on operating leadership accounts. Secretariat entities operated accounts in the name of their senior officials which were supported by the social media teams of the entity. For example, DPPA considered the 'X' social media account in the name of the Under-Secretary-General as an institutional account. On the other hand, the Department of Peace Operations provided support to 24 social media accounts of their leadership but considered them as the senior managers' personal social media accounts. Some of these accounts carried official titles, the United Nations flag and emblems, but they did not indicate whether the posts were made in a personal capacity. Further, since these accounts were not required to be registered in the central database of institutional social media accounts maintained by DGC, they were not subject to safeguards such as risk analysis, purpose and control of these accounts. The guidelines for senior staff and spokespersons on using social media accounts were last updated in 2012. Those guidelines had been expanded for only for one social media platform – X.

(c) Use of verified social media accounts – Due to the increasing number of fake accounts and the risk of misinformation and disinformation³, organizations make efforts to obtain a “verified” status on the most popular social media platforms such as X and Meta (Facebook, Instagram, WhatsApp), since “verified” status proves the authenticity of the account. Currently, there is no policy or guidance requiring entities to obtain “verified” status, leading to inconsistent approaches within the Secretariat. For example, the @UN X account had a verified status, while @UN_OpSupport account of the Department of Operational Support did not. Similar accounts such as @UNGACM_EN, @UN_Mappers, @UNYearbook and @UNLibrary were unverified. Additionally, some of the WhatsApp accounts operated by UNICs which were created as personal accounts were not in “verified” status. DGC stated that due to the rapidly changing social media landscape, it was not feasible to have an institutional policy on the use of verified social media accounts. OIOS is of the view that the “verified” vis-a-vis unverified social media accounts could be considered as part of the risk analysis required at the time of establishing a social media account.

(d) Privacy impact assessment of social media accounts – OIOS' advisory review report on the management of data classification and data privacy in the United Nations Secretariat (DGC-2020-015) had recommended that DGC should establish procedures and controls to monitor United Nations social media accounts. During the present audit, DGC stated that it did not accept the OIOS recommendation because there was no tool that could monitor content being posted for sensitive or personally identifiable information. DGC shared the social media guidelines published in June 2011 by the former Department of

³ Misinformation is false information that is spread with no intention of harm (Wardle and Derakhshan, 2017). Disinformation is false information that is spread with an intention to harm (Wardle and Derakhshan, 2017)

Public Information which aimed to protect the privacy of individuals, including colleagues depicted in social media materials. Also, there was no social media privacy notice published on the United Nations website.

(e) Lack of formal support mechanisms between DGC and Secretariat entities on social media – While informal support channels exist whereby DGC assists the entities in following up with social media platforms, there were no specific support provisions defined. For example, in one instance, DGC supported an entity in unblocking its social media platform, but in another instance related to an imposter social media account, DGC advised the affected department to contact the social media platform directly. Unclear support mechanisms could result in delays and make the problem-resolution process ineffective.

(f) Use of messaging for social media platforms – There was no policy on whether institutional social media accounts should be enabled to receive user messages. DGC stated that it advises entities not to enable messaging unless there is staffing in place to respond to messages, or there is an approved messaging ‘bot’ set up for this purpose. OIOS’ review showed no defined parameters based on which messaging would be enabled or otherwise on a social media account. For example, the Snapchat account of @UN was enabled for chats, but no response was sent to the messages received on this account. Messages sent to @Vistun X account took a few hours to up to 14 days to receive a response. Lack of a timely response could result in poor user experience. There was also a need for an Organizational policy on how the individual messages would be managed, and whether they would need to be preserved for any future use.

(g) User blocking on social media platforms – There was no policy on blocking of users on institutional social media platforms. Social media managers across the Secretariat blocked users they deemed to be spreading disinformation or hate, or improperly using the platform. User blocking and unblocking, in the absence of an institutional policy, could be considered inappropriate or excessive.

(h) Terms of use – Best practice recommends that an organization develop and publish its social media terms of use for the managers of its institutional social media accounts. The terms of use should include components such as platform privacy policies, account security, user conduct, indemnification and termination. Social media accounts were established in a personal capacity by accepting the default terms and conditions of the platform. The Office of Legal Affairs (OLA) did not review such “click and accept” type of agreements. It is notable that the Organization had an agreement with only one social media platform. DGC and OLA stated that obtaining such institutional agreements with social media platforms was very difficult. Given this situation, it is important for the Organization to formalize its terms of use for managers of institutional social media accounts.

17. *DGC stated that changing a Secretary-General’s bulletin is an enormously difficult and lengthy endeavour, and the changes requested do not warrant such a lengthy and difficult process.* OIOS suggests that DGC consider the above-mentioned issues for strengthening the Secretary-General’s bulletin on the institutional use of social media in future revisions.

B. Governance and policy framework for websites

Need to establish a web steering committee

18. It is best practice for organizations to have a forum to oversee and coordinate cross-functional issues related to website governance and oversight, establish key success factors, and provide a forum to discuss and resolve cross-functional issues.

19. The Secretariat did not have a committee or similar body to oversee and coordinate website governance and compliance with the administrative instruction ST/AI/2022/2 on website publishing. Given that the Secretariat had more than 760 public websites across various entities, a web steering committee would help to coordinate key issues among DGC, OICT and the Secretariat entities on matters related to website publishing including security, hosting, architecture and compliance with the standards on website publishing. DGC stated that there were proposals to establish a web steering committee.

Need to ensure compliance with ST/AI/2022/2

20. ST/AI/2022/2 on website publishing established a central registry for websites on uniteapps.un.org. The registry listed United Nations websites including their details, names of focal points, and compliance status with established website publishing standards. OICT was designated as the custodian of the website registry. Additionally, the administrative instruction established a website portfolio under the custodianship of DGC containing details of all United Nations websites, names of focal points including those with access and posting rights, and compliance with the established standards for branding, multilingualism, accessibility, analytics tracking, domain usage, and long-term preservation of content. The administrative instruction also established roles and responsibilities for DGC, OICT and the entities for website publishing and maintenance. OIOS noted the following:

(a) DGC's portfolio of websites was incomplete and did not have any correlation with the website registry maintained by OICT. The portfolio maintained by DGC contained a listing of 206 websites as compared to 764 on the OICT registry on Unite Apps. While the Unite Apps registry contained the names of the website focal points, it did not provide information on all individuals responsible for posting content on the websites. DGC's website portfolio was expected to be a complete, approved and authentic source of all United Nations websites, while the website registry maintained by OICT was expected to serve as a monitoring mechanism for compliance with website standards. In the absence of a link between the two, the authenticity, completeness and validity of the website database was not verifiable. DGC stated that Unite Web and the web portfolio are currently two separate technical entities, and it has no input or control over Unite Web and does not have the resources to manage all the web presences on Unite Web.

(b) DGC did not undertake any annual survey to ensure that the website portfolio was complete and updated. Although entities had the responsibility to communicate any changes to their websites to DGC, there were no monitoring and follow-up mechanisms to ensure that the entities submitted this information. Incomplete information could prevent effective use of the website portfolio.

(c) DGC had established a form (DGC.8) for use by Secretariat entities to request a public website in the un.org domain. The form also specified multilingualism as a key requirement for website publishing. This form was the basis for review and approval of any website with reference to publishing standards such as branding, accessibility, authority, content and multilingualism. Without the approved form, no United Nations website was authorized to be published. DGC's website portfolio contained only 206 DGC.8 forms out of 764 public websites. It could not be confirmed whether all the public websites complied with website publishing standards. Regarding multilingualism, exception approval (temporary and permanent) was required from DGC for deviation from the standards on multilingualism. While the requests were initially approved or denied by DGC, there was no follow-up mechanism to ensure that the websites that were granted temporary exceptions on multilingualism complied with their obligation on the expiry of the exception period. For example, the multilingual status of 97 (out of 121) websites that were marked as multilingual in form DGC.8 could not be verified. Similarly, the DGC.8 form for requesting a public website required compliance with the implementation of a standard tracking code provided by DGC on all public websites for accurate data collection and analytics. However, compliance with this requirement was not ensured (such as the un.org subdomain – research.un.org, unmultimedia.org and www.ungsc.org).

(d) DGC had developed two other forms - DGC.7 (Request for SFTP access and posting rights) and DGC.9 (un.org website branding code – an agreement not to share or modify DGC web branding styling, code and assets). However, these forms were not used. DGC’s website portfolio contained only 27 DGC.7 forms and one DGC.9 form, which showed that the information on posting rights as required by ST/AI/2022/2 was incomplete, and so was the requirement for compliance with the branding code. Further, there was no process to ensure the collection of the missing forms.

(e) All non-un.org domains were expected to be registered with DGC indicating details and purpose of the website. A form was established by DGC for this purpose on the intranet (<https://iseek.un.org/content/non-unorg-domain-name-registration-form>) in accordance with the standards for website publishing. As of May 2023, only 38 non-un.org domains were registered with DGC through this form. The web registry maintained by OICT contained 562 non-un.org public websites for which there was no entry in the DGC website portfolio. ST/AI/2022/2 requires the submission of registration forms for all non-un.org websites to DGC. This condition could lead to ineffective and inadequate control over the creation of websites that are not un.org subdomains or subdirectory websites.

(3) DGC, in coordination with OICT and the respective Secretariat entities, should work to raise the awareness of and requirements for compliance with website governance.

DGC accepted recommendation 3.

C. Content management

21. Content management is the process of collection, delivery, retrieval, governance, accessibility, branding and overall management of information on websites and social media platforms. Content management includes the administration of the digital content lifecycle from creation to permanent storage or deletion. The content could include text, images, videos and multimedia. Content management also requires that posting rights for the content are adequately managed. OIOS noted the following:

Lack of a centralized database on posting rights

22. ST/AI/2022/2 as well as ST/SGB/2019/5 require that Secretariat entities communicate to DGC the names of their authorized staff with posting rights for websites and social media platforms. Currently, these databases were not updated, and there was no process to ensure their completeness. Implementing recommendation 2 above should help address this condition.

Need to assign resources for compliance with website accessibility standards

23. The United Nations web building guidelines published by DGC require compliance with web branding guidelines and accessibility standards across the websites so that the United Nations’ digital presence has a consistent look and feel and is accessible to all. In paragraph 5 of its resolution 61/106 on “Convention on the Rights of Persons with Disabilities”, the General Assembly requested the Secretary-General to progressively implement standards and guidelines for accessibility of facilities and services of the United Nations system. OIOS is of the view that accessibility to services includes accessibility to the Organization’s websites in terms of the Web Content Accessibility Guidelines (WCAG) of the World Wide Web Consortium Web Accessibility Initiative (W3C WAI).

24. Presently, there were lack of resources and tools to ensure compliance with accessibility standards. OIOS noted the following:

(a) While DGC had published web guidelines and accessibility standards, the Organization lacked the standard tools and resources to monitor compliance of all publicly accessible websites. DGC used WCAG to check for accessibility of the requested websites, but this process was manual and resource-intensive. Public websites such as <https://www.un.org/africarenewal/>, <https://psdata.un.org/> and unmissions.org lacked compliance with the branding standards. Similarly, OIOS' review of eleven websites using publicly available accessibility review tools showed that accessibility standards were not fully met by these websites. DGC stated that it lacked the capacity to ensure periodic checks on websites for compliance with accessibility and branding. Additionally, DGC typically gets access to one language version of the website during the development phase, so it does not check compliance across all six languages. Moreover, DGC may not be informed in case the site is redesigned using the same URL.

(b) The intranet iSeek, which is an important source of information for all staff, was excluded from the accessibility standards. Similarly, some websites such as the United Nations' career portal (careers.un.org) were excluded from the definition of public websites even though they remained an important source of information for career aspirants. The careers website had 5.78 million visits between April to June 2023, with 778,891 unique visitors every month.

(4) DGC should assign resources to ensure compliance with the website accessibility standards for the Organization's public websites.

DGC did not accept recommendation 4 stating that it is not in a position to assign resources. OIOS notes that compliance with website accessibility standards by the Organization's public websites is required for providing accessibility to persons with disabilities. This unaccepted recommendation has been closed based on Management's acceptance of the residual risks.

Need for a policy on consent management for websites

25. Best practices require compliance with good data privacy practices. The Secretary-General's Data Strategy emphasises data privacy and data protection across the Secretariat. The current privacy notice posted on the United Nations website (www.un.org) was generic and outdated. Further, United Nations websites did not currently employ a user consent system to inform the visitors of the tracking and analytic tools used to track user behaviour and seek permission for not strictly needed tracking tools and cookies. There was also no process to check for the tracking cookies implemented on the Secretariat's public websites. For example, while un.org did not employ tracking cookies, websites such as library.un.org and news.un.org had tracking cookies which were not strictly necessary.

26. DGC stated that it has worked extensively with OLA to develop and finalize a new data protection and privacy notice in line with the Data Strategy. This work was completed in 2021. DGC also stated that the publishing of the new data protection and privacy notice has been put on hold until the new "United Nations Data Protection Officer" has been recruited and on-boarded.

Need to ensure compliance with archiving and preservation of web content

27. ST/AI/2022/2 describes procedures for archiving and preservation of content from retired United Nations websites. The retired website must be deposited with United Nations libraries, digital preservation, and permanent public access in accordance with ST/AI/189/Add.12/Rev.1 – Regulations for the control and limitation of documentation. According to ST/AI/2022/2, the library must be consulted when a website is retired so that the content of the website, including all forms of digital publications thereon, are captured and preserved. OIOS noted the following:

(a) There was no process to ensure that Secretariat entities complied with ST/AI/2022/2 for archiving their retired websites. The library had designed a form for entities to communicate the need for retired website preservation, but this form was yet to be implemented. Additionally, there was no status field in the Unite Apps website registry to indicate which of the websites were archived. There were 430 retired public websites in the Unite Apps portal. OIOS' review of 10 retired websites showed that five were still active. This was also the case with websites that belonged to other entities (e.g., the retired Accounts Division Portal with web link as <http://ppbd.un.org/default.asp>).

(b) The United Nations Library used a tool to crawl 270 public websites to capture textual content (digital files) for preservation purposes. However, websites currently crawled did not include websites marked as retired in the website registry. Only three retired websites from Unite Apps were included in the archived site list of the library⁴. The library stated that it did not have the resources, tools or mandate to scan Unite Apps for retired websites to evaluate and archive their digital content.

Need for procedures to preserve information posted on social media accounts

28. ST/SGB/2019/5 on the institutional use of social media did not include provisions for archiving the Organization's social media accounts. Presently the library crawled 20 X accounts related to Under-Secretaries-General, Assistant Secretaries-General and special envoys creating a dark archive for purely research purposes (not accessible publicly). However, social media accounts other than X were not crawled/archived. Similarly, the Organization's own institutional X accounts such as @UnitedNations were not included in the archive list. The library stated that the changes in X leadership have impacted public access to content posted on their platform, which may impact the archiving of tweets. Therefore, the library plans to deprioritize the archiving of such tweets. Similarly, there was no procedure to ensure business continuity in case the accounts were blocked by the platforms. For instance, a Secretariat entity faced a situation where its account was blocked by the platform twice. This situation showed that in case the account is not released or is permanently blocked, all information on that account would be lost and would need to be recreated.

29. This condition occurred because the Secretariat had yet to define procedures for archival of social media content in line with the Secretary-General's bulletin ST/SGB/2007/5 on Record keeping and management of United Nations Archives. Lack of procedures to archive social media content could result in loss of valuable information of potentially historical importance. DGC stated that it could provide standards and best practices regarding metadata creation of social media. However, the ability to archive content is dependent on the policies of third-party platforms. It is not possible to archive social media due to technical restrictions put in place by these platforms. Recent changes at X, for instance, have ended the previously large-scale archiving of content on its predecessor platform.

(5) DGC, in coordination with OICT, should undertake a capacity assessment and establish a process for decommissioning websites in accordance with ST/AI/2022/2.

DGC accepted recommendation 5 and stated that its implementation will be contingent on receiving additional funding.

⁴ <http://www.un.org/en/events/slaveryremembranceday/>, <http://www.un.org/millenniumgoals/> and <https://blogs.un.org/unstories/>.

D. Security of websites and social media

Need for strengthening independent security assessment for websites

30. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(6) OICT should establish a process for periodic independent security assessment for the Secretariat's websites with a focus on remediation of the already identified ICT security vulnerabilities.

OICT accepted recommendation 6.

Need to strengthen controls over the monitoring and detection of fake social media accounts and websites

31. The Secretariat currently did not have adequate procedures and tools to detect and act on fake accounts and websites. A protocol for handling hybrid cyberattacks was prepared by the transition team of the Executive Office of the Secretary-General which contained protocols on handling forged social media accounts and fake websites (public impersonation). The protocol document required DGC to lead a coordinated response after assessing the impact of fake social media accounts and fake websites from a reputational perspective and devise an appropriate response within 24 hours. OIOS noted the following:

(a) The hybrid cyber response team protocol was not finalized. DGC and OICT stated that the current arrangement was informal without any specific terms of reference. There was no evidence that a capacity assessment was done of the resources and tools required for such an operation.

(b) DGC did not maintain a database for fake social media accounts. During the audit, OIOS brought two fake social media LinkedIn accounts and two websites to the notice of DGC and OICT. Tools such as

Proofpoint Social Discover could be used to detect persistent fake social media accounts. Given that social media accounts are vulnerable to hacks, phishing and takeovers, the static lists of user accounts and manual monitoring of content may not be adequate for medium and long-term needs.

(c) DGC maintained a registry of actions taken on fake and imposter websites. From March 2021 till July 2023, 23 actions were recorded in the DGC database for forgery of United Nations websites. OIOS also obtained information from OLA for the period January 2022 to May 2023 which showed that a ‘cease and desist’ notice was issued in five cases, and takedown requests were issued in four other cases. OLA stated that the number of notices of ‘cease and desist’ and takedown requests issued by OLA during the period concerned misuse of the United Nations’ name and emblem on websites, social media platforms and email, and did not include cases where the misuse was taking place only in ‘hard copy’ communications and/or documents. Additionally, there were cases under review by OLA that were not included in the statistics of ‘cease and desist’ notices and takedown requests issued.

(d) There was lack of a comprehensive and shared database that could be used by DGC, OLA and OICT to track the response to fake websites. Three imposter sites last detected in 2021 were still active as of date. Ad hoc and manual detection and lack of timely response may not be effective in protecting the Organization from risks that may impact its reputation.

(7) OICT, in collaboration with DGC and other Secretariat entities, should finalize the protocol of the hybrid cybersecurity response team with clear terms of reference, roles and responsibilities, and actionable timelines.

OICT accepted recommendation 7.

Lack of policy on the use of multi-factor authentication for social media accounts

32. Social media accounts could be subject to hacking, hijacking and denial of service attacks by unauthorized personnel, who could use the accounts to propagate false information thereby damaging the credibility of the Organization.

33. Multi-factor authentication (MFA) is a best practice for mitigating such risks. While MFA is a standard norm for most business applications in the Secretariat, its enablement for social media differs from platform to platform and from one account to another. The Secretary-General’s bulletin does not clearly specify the authentication and password requirements for social media platforms. Currently, it was not possible to enumerate which of the social media accounts were enabled for MFA. Such information was not designed to be collected in the DGC registry or elsewhere. It is essential to identify the social media accounts that are not enabled for MFA so that additional controls can be instituted around them. Similarly, it is necessary to specify a password policy for institutional social media accounts across the Secretariat.

(8) DGC should define guidelines for the use of multi-factor authentication across social media accounts.

DGC accepted recommendation 8.

E. ICT support

Need to expedite implementation of an integrated web communications platform

34. Good practice recommends that an organization maintains an integrated web communication platform to ensure compliance with its web publishing standards. Such a platform was not yet deployed in the Secretariat. DGC stated that it has been working with OICT on a project to establish a global web communications platform (UN3 integrated web communications platform) in the six official languages as well as regional and local languages as used by various DGC communication programmes. UN3 will be compatible with the latest version of the Secretariat's standard web technology (version 8/9 of Drupal) and provide improved centralization of presently fragmented web presences. An integrated and centralized platform is expected to ensure compliance with United Nations web communication standards such as web branding, accessibility and multilingualism. However, this project was significantly delayed from its original timeline of April 2022. Establishing a common platform for building the Secretariat's websites would automatically ensure compliance with branding and accessibility.

(9) OICT, in coordination with DGC, should prioritize the implementation of the UN3 integrated web communications platform to improve compliance with website publishing standards and address the presently fragmented web presence.

OICT accepted recommendation 9.

Need for an automated tool for websites and social media

35. Best practices require that an organization regularly reviews its website portfolio to eliminate content defects, missing web links, and duplication of content. Such reviews also assist in search engine optimization to increase website traffic and track website rankings.

36. There was lack of Organization-wide ICT standards for social media analytic tools (such as Talkwalker tool). The tool currently used by DGC and some other Secretariat entities for social media analytics was not vetted through the Architecture Review Board of OICT. The lack of standards could cause inconsistency, duplication and suboptimal use of such tools across the Organization.

37. OIOS used a readily available tool to scan 100 pages on the flagship website and identified multiple errors and warnings including duplicate content across pages, duplicate title tags, broken internal JavaScript files, pages with duplicate meta descriptions, and broken links. Manual scanning of websites is inefficient and impractical given the number of webpages and websites, thus requiring consideration and use of automated scanning tools.

38. The library did not have automated tools and capacity for archiving a large number of digital files because it required resources for metadata creation and quality control of the massive amount of content (e.g., 7,000 digital files in one month). The current process was manual and resource-intensive, which necessitates an assessment for implementing automated tools for website archiving by the library.

39. There were no dashboards to track the use of social media platforms across the Secretariat. Dashboards reflecting the status of social media accounts entity-wise could provide useful information on the compliance and verification status of such social media accounts.

(10) DGC should assess the requirements for automated tools to monitor the Secretariat's websites and social media accounts.

DGC accepted recommendation 10.

IV. ACKNOWLEDGEMENT

40. OIOS wishes to express its appreciation to the Management and staff of DGC, OICT and the Secretariat's entities for the assistance and cooperation extended to the auditors during this assignment.

Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of management and security of websites and social media in the United Nations Secretariat

Rec. no.	Recommendation	Critical ⁵ / Important ⁶	C/ O ⁷	Actions needed to close recommendation	Implementation date ⁸
1	DGC should strengthen the framework for governance and management of social media in the Secretariat by: (a) developing guidelines for Secretariat entities on strategies and use of social media in furtherance of their mandates; and (b) establishing a committee or similar body for coordination and review of the social media needs of the Secretariat.	Important	O	Receipt of evidence of action taken to strengthen the framework for governance and management of social media in the Secretariat.	31 December 2024
2	DGC should undertake an annual campaign to ensure the upkeep and completeness of the social media database in accordance with the Secretary-General's bulletin on the institutional use of social media in the Secretariat.	Important	O	Receipt of evidence of undertaking an annual campaign to ensure the upkeep and completeness of the social media database.	30 June 2024
3	DGC, in coordination with OICT and the relevant Secretariat entities, should work to raise the awareness of and requirements for compliance with website governance.	Important	O	Receipt of evidence that DGC has coordinated with OICT and relevant Secretariat entities to raise the awareness of and requirements for compliance with website governance.	31 December 2024
4	DGC should assign resources to ensure compliance with the website accessibility standards for the Organization's public websites.	Important	C	This unaccepted recommendation has been closed based on Management's acceptance of the residual risk.	Not implemented
5	DGC, in coordination with OICT, should undertake a capacity assessment and establish a process for decommissioning websites in accordance with ST/AI/2022/2.	Important	O	Receipt of evidence that DGC has undertaken a capacity assessment and established a process for decommissioning websites in accordance with ST/AI/2022/2.	31 December 2024
6	OICT should establish a process for periodic independent security assessment for the	Important	O	Receipt of evidence that OICT has established a process for periodic independent security	31 March 2025

⁵ Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

⁶ Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

⁷ Please note the value C denotes closed recommendations whereas O refers to open recommendations.

⁸ Date provided by DGC and OICT in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of management and security of websites and social media in the United Nations Secretariat

	Secretariat's websites with a focus on remediation of the already identified ICT security vulnerabilities.			assessment for the Secretariat's websites with a focus on remediation of the already identified ICT security vulnerabilities	
7	OICT, in collaboration with DGC and other Secretariat entities, should finalize the protocol of the hybrid cybersecurity response team with clear terms of reference, roles and responsibilities, and actionable timelines.	Important	O	Receipt of evidence that OICT, in collaboration with DGC and other Secretariat entities, has finalized a protocol of the hybrid cybersecurity response team with clear terms of reference, roles and responsibilities, and actionable timelines.	31 March 2025
8	DGC should define guidelines for the use of multi-factor authentication across social media accounts.	Important	O	Receipt of evidence that DGC has defined guidelines for the use of MFA across social media accounts.	30 June 2024
9	OICT, in coordination with DGC, should prioritize the implementation of the UN3 integrated web communications platform to improve compliance with website publishing standards and address the presently fragmented web presence.	Important	O	Receipt of evidence that OICT has prioritized the implementation of the UN3 integrated web communications platform to improve compliance with website publishing standards and address the presently fragmented web presence.	31 December 2024
10	DGC should assess the requirements for automated tools to monitor the Secretariat's websites and social media accounts.	Important	O	Receipt of evidence that DGC has assessed the requirements for automated tools to monitor the Secretariat's websites and social media accounts.	30 June 2024

APPENDIX I

Management Response

TO: Mr. Byung-Kun Min, Director
A: Internal Audit Division, OIOS

DATE: 27 December 2023

REFERENCE: OIOS-2023-02200

CLASSIFICATION: Unclassified

FROM: Ms. Melissa Fleming, Under-Secretary-General
DE: Department of Global Communications



SUBJECT: **Draft report on an audit of management and Security of websites and social media in the**
OBJET: **United Nations Secretariat (Assignment No. AT2022-580-01)**

1. With regards to your memorandum dated 5 December 2023, transmitting the draft report on the audit of management and security of websites and social media in the United Nations Secretariat, please find attached the completed Appendix I with DGC's comments.
2. Kindly note that comments from OICT and OLA were also incorporated in the Appendix.
3. DGC is grateful for OIOS's work on this review.
4. Thank you.

cc: Mr. Travis Weyer
Ms. Janet Wieser

**Audit of management and security of websites and social media in the United Nations Secretariat
Management Response – Appendix I**

Rec No.	Recommendation	Critical/ Important	Accepted (?) (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	DGC should strengthen the framework for governance and management of social media in the Secretariat by: (a) developing guidelines for Secretariat entities on strategies and use of social media in furtherance of their mandates; and (b) establishing a committee or similar body for coordination and review of the social media needs of the Secretariat.	Important	Yes	Chief of Social Media/ CCOD	31-Dec-2024	
2	DGC should undertake an annual campaign to ensure the upkeep and completeness of the social media database in accordance with the Secretary-General's bulletin on the institutional use of social media in the Secretariat.	Important	Yes	Chief of Social Media/CCOD	30-June-2024	
3	DGC should formulate guidelines in consultation with the Office of Human Resources on use of social media by non-staff personnel for posting content relating to the United Nations and their official activities.	Important	Yes	Chief of Social Media/ CCOD	31-Dec-2023	Revised social media guidelines for staff and non-staff were issued in July 2023
4	DGC, in coordination with OICT and relevant working groups, should work to raise the awareness of and requirements for compliance with website governance.	Important	Yes	WSS/NMD	31-Dec-2024	Suggestion to amend the recommendation as follows: DGC and OICT, in coordination with respective Secretariat entities, should work to raise the awareness of and requirements for compliance with website governance.

5	DGC should assign resources to ensure compliance with the website accessibility standards for the Organization's public websites.	Important	No			The Department is not in a position to assign resources.
6	DGC, in coordination with OICT, should undertake a capacity assessment and establish a process for archiving websites in accordance with ST/AI/2022/2.	Important	Yes, with changes (see reformulation request)	DHL/OD	31 Dec. 2024	<p>The implementation of this recommendation in the current formulation would be strictly subject to receiving additional funding. As previously noted, the Department does not have the capacity to archive the whole of websites (incl. multimedia, videos, photos etc.) or the website itself since that would require data storage the Department cannot afford.</p> <p>Therefore, we would request the following edit: <i>DGC, in coordination with OICT, should establish a process for decommissioning websites in accordance with ST/AI/2022/2.</i></p>
7	OICT should establish a process for periodic independent security assessment for the Secretariat's websites with a focus on remediation of the already identified ICT security vulnerabilities.	Important	Yes	Chief, Cyber Security Service, OICT	31 March 2025	
8	OICT, in collaboration with DGC and other Secretariat entities, should finalize the protocol of the hybrid cybersecurity response team with clear terms of reference, roles and responsibilities, and actionable timelines.	Important	Yes	Chief, Cyber Security Service, OICT	31 March 2025	
9	DGC should define guidelines for the use of multi-factor authentication across social media accounts.	Important	Yes	Chief of Social Media	30-June-2024	

10	OICT, in coordination with DGC, should prioritize the implementation of the UN3 integrated web communications platform to improve compliance with website publishing standards and address the presently fragmented web presence.	Important	Yes	Chief, EAC- Americas	31-Dec-2024	
11	DGC should assess the requirements for automated tools to monitor the Secretariat's websites and social media accounts.	Important	Yes	ECRU/OUSG	30-June-2024	

United Nations  Nations Unies


INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

TO: Mr. Byung-Kun Min, Director
A: New York Audit Service
Internal Audit Division, OIOS

DATE: 22 December 2023

THROUGH: 
Christophe Monier
S/C DE: Director, Business Transformation and Accountability Division
Department of Management Strategy, Policy and Compliance

FROM: 
Mario Baez
DE: Chief, Accountability Service
Business Transformation and Accountability Division
Department of Management Strategy, Policy and Compliance

SUBJECT: **Draft report on an audit of management and security of websites and social media**
OBJET: **in the United Nations Secretariat (Assignment No. AT2022-580-01)**

1. With reference to your memorandum dated 5 December 2023, please find attached Appendix I with comments provided by the Department of Management Strategy, Policy and Compliance (DMSPC) on the OIOS recommendations. Additionally, please find below general comments from the Office of Legal Affairs (OLA).

General comments

2. OLA had an interview with OIOS concerning the subject matter of this audit and provided some information on relevant points. In addition, at OIOS' request, OLA reviewed and provided comments on the prior drafts of this audit report.

3. OLA has noted with thanks that OLA's previous comments have been reflected in the Draft Report except for one concerning paragraph 33 (c) of the Draft Report which provides, inter alia, that "OIOS also obtained information from OLA for the period January 2022 to May 2023 which showed that a 'cease and desist' notice was issued in five cases, and takedown requests were issued in four other cases."

4. In previous comments by OLA, it had indicated to OIOS that the number of the notices of cease and desist and takedown requests issued by OLA during the relevant period (i.e., January 2022 to May 2023) concerned misuse of the UN name and emblem on websites, social media platforms and e-mail, and did not include the cases where the misuse was taking place only in 'hard copy' communications and/or documents. OLA also noted that the cases that were under review by OLA had not been included.

5. In this regard, OLA would like to reiterate that OIOS may wish to consider including the above-referenced clarification in the final audit report.
6. Thank you for giving the Administration an opportunity to provide comments on the draft report.