

REPÚBLICA DEMOCRÁTICA  DE SÃO TOMÉ E PRÍNCIPE

AFAP – Agência Fiduciária de Administração de Projectos

Ministério das Finanças de Economia Azul

PROJETO DIGITAL DE SÃO TOMÉ & PRÍNCIPE

Comentários e Respostas do BM e do Consultor, respectivamente sobre o Plano de Gestão de Resíduos (PGR) e Avaliação do Risco de Segurança (ARS)

Plano de Gestão de Resíduos (PGR)

N.º	Comentário	Resposta
1	Background and purpose: General best practices in handling E-waste are presented but without providing any context or sufficient background in terms of how waste in general (i.e. both hazardous and non-hazardous, including domestic and e-waste) is managed in STP. Please provide more specific information (potential sites of final disposal, temporary storage facilities, tracking methods of the sub-contractors who will dispose the waste etc.).	A whole new Chapter 4 has been developed to include all relevant background that is possible to put together using the existing and relevant information
2	Structure and content: The document does not have to repeat the project description, budget, describe beneficiaries, etc. and should instead be more objective and focused on presenting a diagnostic of the current operational systems of solid waste collection, transport, triage/storage and final disposal in STP (including e-waste) or elsewhere, upon which the project may or may not need to rely for disposing of e-waste, based on an analysis of alternatives and/or suitable strategies for end-of-life disposal. WB Requirements of ESS3 on waste management must be more clearly demonstrated. ESS 3 states that the Borrower will minimize the generation of waste, and reuse, recycle and recover waste in a manner that is safe for human health and the environment. Please refer to WB Guidance Note on ESS 3	Repeated chapters taken out. See point 1, above, about diagnostics and background. Potential synergies that can be established between PD-STP and other existing initiatives in STP also better specified. Box 4.1. WB waste management framework, which was already in the previous version, contains the essential elements of ESS3 re WMF. Critical aspects showing the sequence of steps to be followed underlined.

N.º	Comentário	Resposta
	<p>(https://documents1.worldbank.org/curated/en/112401530216856982/ESF-Guidance-Note-3-Resource-Efficiency-and-Pollution-Prevention-and-Management-English.pdf)</p> <p>Please note that the WMP document contains some potential discrepancies with established best practices in solid waste management (cf. Tabela Tabela 4-1: Principais instrumentos do quadro legal santomense na gestão de resíduos: que estabelece a seguinte hierarquia a) Aterro sanitário; b) Incineração; c) Compostagem; d) Reciclagem). It would seem that the steps in this national waste management hierarchy are reversed, please revise.</p>	<p>STP Decree on waste management (Definitions) presents the WM hierarchy as stated in the document. A note has been made to indicate that this could be misleading, and the right sequence restated in line with what is in Box 4.1. WB waste management framework</p>
3	<p>Institutional arrangements: Currently the document does not allow for an understanding of how solid waste is managed overall in STP, making it difficult for the project executing agency/ies (e.g. PIU) to identify deficiencies and opportunities to address waste chain logistics and infrastructure bottlenecks. Please add a table describing the roles and responsibilities of each institution in executing the WMP. Given that the WMP will be used as a guide for project contractors to adapt their own WMP, it will be important to explain how the sector is organized in STP: whether public and/or private operators are involved, approximate volumes, collection/triage/storage points, gaps in service/area coverage, destinations (e.g. landfills, recycling, reuse, etc.), if any of those are in fact available. If STP has only one functioning (hospital) incinerator for disposal of biohazardous and other hazardous materials, then the WMP would ideally also include a short needs assessment analysis in terms of infrastructure/equipment upgrades required in order to accommodate higher volumes of waste, if needed. Also, it would be important to ascertain whether any transboundary movement of e-waste is taking place involving STP and, if so, if the movement of these hazardous and non-hazardous waste is being done in accordance with the Basel Convention's Technical Guidelines (Addendum - Technical guidelines on transboundary movements of electrical and electronic waste and used electrical and electronic equipment, in particular regarding the distinction between waste and non-waste under the Basel Convention:</p>	<p>Subchapter 3.1.1.2 Waste Management now presents a more specific institutional framework for WM, while Chapter 4 (see above) presents the overall context in which WM is done in STP including the various initiatives with which PD-STP can establish lines of collaboration and synergies after assessments and needs identification. These are not limited to the hospital.</p> <p>While there is no evidence that there have been transboundary waste movements in STP there are wastes that have been stored for potential export. PD-STP is required to get more details about that and see the extent to which they can benefit the project.</p>

N.º	Comentário	Resposta
	http://www.basel.int/Portals/4/download.aspx?d=UNEP-CHW.14-7-Add.6-Rev.1.English.pdf), which entered into force in STP in 2014.	

Avaliação do Risco de Segurança (ARS)

N.º	Comentário	Resposta
1	<p>Background and purpose: The document does not have to repeat the project description, budget, etc. and could instead be more objective and focused on proposing/outlining security management guidelines and measures proportionate to the nature and magnitude of the security risks and threats identified – including emergencies. Although the perceived overall security and threat acute risk is relatively low, the document needs to put forward a more detailed basis for addressing the threats to project personnel, assets, and affected communities.</p>	
2	<p>Content: the SRA presents a general introduction of the security context in STP, based on secondary data including official reports, media articles, and literature. However hard data is quite limited/partial (literature references to GBV and domestic violence date to 2004) and presented in absolute terms (section 4.1), and hence it's not possible to establish a comparable basis with statistics from other country settings with which to develop/apply suitable mitigation measures to prevent the exacerbation of those risks. For instance, the document reports a potentially very significant increase in cases of GBV/SEA in 2019 and 2020, but proposes that root causes may be related to greater awareness and/or increased reporting, not putting forward the incidence of COVID-19 and social distancing as potential intervening factors. Hence, the document lacks some more details on the project's social and political context, security-related risks, and potential risks posed by use of security personnel – all of which would inform the need for a dedicated Security Management Plan or not (e.g. subsumed within the ESIA process). The SRA does not propose any mitigation management measures and is unclear on whether a SMP will be needed. In section 1.2 (ARS) there is text from a 'WB Good Practice Note on Assessing and Managing the Risks and Impacts of the Use of Security Personnel Bank' that refers to steps and sources for WB project teams to follow during appraisal to obtain an initial understanding of a project's security risks (regarding type, location, and the political context in the country); hence, these are not necessarily elements of an SRA itself. In section 2.13 (Arranjos de Implementacao), a long list of implementing institutions and the general institutional set up is presented but it's not clear if all will be involved/to what extent in management of security-related issues</p>	

N.º	Comentário	Resposta
	<p>(i.e. roles and responsibilities), whereas some relevant institutions are missing including National Civil Defense Service, Fire Department, and Coast Guard. It is understood -but not specified- that the safeguards specialists of the PIU at AFAP will be in charge of overseeing overall borrower management of security issues pertaining to ESS1, ESS2 and ESS4. Table 3.1: remove reference and text to ESS9, as it is not relevant to the SRA. There are a couple of additional useful references on SRA in terms of use of private security contractors: i) Use of Security Forces: Assessing and Managing Risks and Impacts (https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces); and ii) The Voluntary Principles on Security and Human Rights (https://www.voluntaryprinciples.org/).</p>	
3	<p>Structure: The SRA is not structured to respond/address some key aspects, namely: i) which security public policies, plans and procedures are needed to safeguard personnel, property and assets given the articulated threat/risk setting (i.e. is the current framework in place adequate?); ii) which operational security protocols may be needed/to be developed by the PIU/contractors; iii) what level of liaison/intelligence gathering activity is warranted with local law enforcement agencies; iv) whether a security guard contractor will be needed for the project based on the main identified threat/risk levels; v) which crisis/emergency management and incident response protocols may need to be developed; v) identify which disaster recovery/business continuity plans may be necessary; and vi) identify security training and capacity building needs and tools. It is suggested to state upfront the main objectives of the SRA i.e: i) identify inherent security risks to the Project, including contextual risks that may affect the Project's effective management of security; ii) identify potential risks (created or aggravated by the Project) to local communities e.g. GBV/SEA; iii) develop risk scenarios; and iv) provide recommendations and guidelines for addressing the identified main risks associated with security management for the project – borrower and contractors.</p>	